

(12) 特許協力条約に基づいて公開された国際

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004年10月28日 (28.10.2004)

PCT

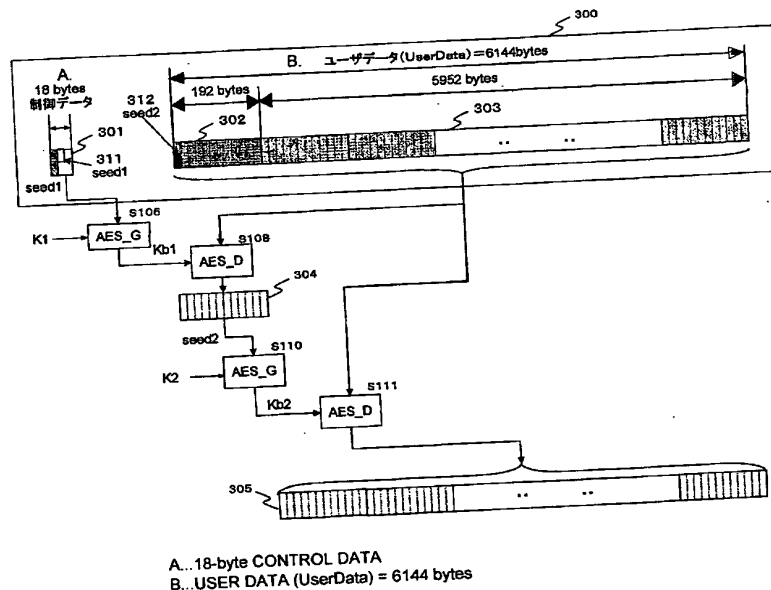
(10) 国際公開番号
WO 2004/093379 A1

- (51) 国際特許分類⁷: H04L 9/08
- (21) 国際出願番号: PCT/JP2004/004909
- (22) 国際出願日: 2004年4月5日 (05.04.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2003-107571 2003年4月11日 (11.04.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 木谷 聡 (KITANI, Satoshi) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 米満 潤 (YONE-MITSU, Jun) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 村松 克美 (MURAMATSU, Katsumi) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 浅野 智之 (ASANO, Tomoyuki) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 高島 芳和 (TAKASHIMA, Yoshikazu) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 宮田 正昭, 外 (MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目1番7号 銀座ティークエビル 澤田・宮田・山田特許事務所 Tokyo (JP).

[続葉有]

(54) Title: INFORMATION RECORDING MEDIUM DRIVE DEVICE

(54) 発明の名称: 情報記録媒体ドライブ装置



A...18-byte CONTROL DATA
B...USER DATA (UserData) = 6144 bytes

(57) Abstract: There is provided a configuration capable of effectively preventing unauthorized use of an encrypted content stored in an information recording medium. Seed information (seed 2) required for generating a block key applied to decryption of the encrypted content is encrypted by a block key (Kb1) and stored. Furthermore, in the configuration requiring transfer of the seed information (seed 2) between devices, both of the seed information (seed 2) and a recording key (K2) are encrypted by a session key before transmission/reception. With this configuration, it becomes difficult to analyze the seed information (seed 2) by data acquisition from the information recording medium and the data transfer path. Thus, it is possible to realize a content protection of a high security level by increasing the difficulty of analysis of key information generated by using the seed information and analysis of the encryption algorithm.

[続葉有]



(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL,

SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 情報記録媒体に格納される暗号化コンテンツの不正利用を効果的に防止することを可能とした構成を提示する。暗号化コンテンツの復号に適用するブロックキーを生成するために必要となるシード情報 (シード2) をブロックキーKb1によって暗号化して格納する構成とした。さらに、シード情報 (シード2) をデバイス間で転送することが必要となる構成において、シード情報 (シード2) および記録キーK2の双方をセッションキーで暗号化して送受信する構成とした。本構成により、情報記録媒体、およびデータ転送路からのデータ取得によるシード情報 (シード2) 解析は困難となり、シード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析困難性を向上させたセキュリティレベルの高いコンテンツ保護が実現される。

明 細 書

情報記録媒体ドライブ装置

5

技術分野

本発明は、情報処理装置、情報記録媒体ドライブ装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。詳細には、情報記録媒体を利用したデータ記録再生処理における不正なコンテンツ利用の防止を実現する情報処理装置、情報記録媒体ドライブ装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。

背景技術

15

昨今、音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはCD（Compact Disc）、DVD（Digital Versatile Disk）、MD（Mini Disk）等の情報記録媒体（メディア）を介して流通している。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、CDプレーヤ、DVDプレーヤ、MDプレーヤ等の再生装置、あるいはゲーム機器等において再生され利用される。

25

音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われなくする構成をとるのが一般的となっている。

特に、近年においては、情報をデジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、

5 不正コピーコンテンツのインターネットを介した配信や、コンテンツをCD-R等にコピーした、いわゆる海賊版ディスクが大量に流通しているという問題がある。

特に、近年開発されたDVD等の大容量型記録媒体は、1枚の媒体に例えば

10 映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。

15 デジタル記録再生を行う記録装置やデジタル記録媒体によれば、画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができ、コピーが違法に行われた記録媒体が市場に流通すると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害され

20 ることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。

例えば、DVDプレーヤでは、コンテンツ・スクランブルシステム(Content Scramble System)が採用されている。コンテンツ・スクランブルシステムでは、DVD-ROM(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いる鍵が、ライセンスを受けたDVDプレーヤに

25 与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従う

ように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

5

一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するための鍵を有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

10

しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体を対象としており、ユーザによるデータの書き込みが可能な記録媒体への適用については考慮されていない。

15

即ち、データの書き込みが可能な記録媒体に記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

20

さらに、CSSの暗号を破るソフトウェアプログラム、例えばDeCSSソフトウェアがインターネット上で配布されており、このプログラムを適用することで、DVD Videoの暗号を解いて平文の状態で記録型DVDへ書き込むことが可能になっている。DeCSSが出現した背景は、本来暗号化が義務付けられているはずのCSS復号用の鍵データを暗号化しないまま設計されたDVDプレーヤー・ソフトウェアがリバースエンジニアされて鍵データが解読されたことであり、解読された鍵データから連鎖的にCSSアルゴリズム

25

全体が解読されたという経緯である。

鍵データを含む著作権保護技術実行プログラムをPC上で実行されるアプリケーションプログラムへ実装する際には、著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的であるが、対タンパー性の強度を示す指標は無く、そのためどれほどリバースエンジニアリングへの対応を行うかは個々のインプレメンターの判断や実力に委ねられているのが実情であり、CSSの場合には結果として破られてしまい、不正なコピーコンテンツの氾濫を招く結果となっている。

CSS以外にも、DVD規格で採用されている著作権保護技術(コピーコントロール技術)として、CPPM(Content Protection for Prerecorded Media)とCPRM(Content Protection for Recordable Media)がある。CPPMは、再生専用のメディア(Prerecorded Media)用に開発されたコピーコントロール技術であり、CPRMは、記録可能なメディア(Recordable Media)用に開発されたコピーコントロール技術である。これらは、メディア(例えばディスク)側にメディアキーブロックと呼ばれる鍵情報を格納し、一方、再生装置、PC等、デバイス側にデバイスキーを格納し、これらの鍵の組み合わせにより、コピーコントロールを行うものである。

しかし、このようなCPRMや、CPPMにおいても、デバイスとしてのPCやメディアとしてのディスク内に格納された鍵情報の漏洩の危険性を解消するといった根本的な問題解決を図る技術についての提案はなく、CPRMや、CPPMにおいても、鍵の漏洩によってコピーコントロールシステムが崩壊する危険性を常に有しているのが現状である。

なお、コンテンツの不正利用を防止する技術として、本出願人は、例えば特許文献1(特許公開2001-351324号公報)および特許文献2(特許公開2002-236622号公報)において、記録媒体に格納するコンテン

5 ツのデータブロック毎に異なる鍵を適用した暗号処理技術を提案した。すなわち、データブロック毎の鍵生成情報としてシードを設定し、ブロック毎に設定したシードを暗号鍵の生成に適用する構成により、従来の1つの鍵のみによるコンテンツ暗号化を複雑化して、暗号アルゴリズムの解読困難性を高めたものである。

10 しかし、上述の構成において、データブロック毎の鍵生成情報としてシードは、記録媒体に格納された情報そのものを使用したものであり、前述のCSSと同様の経緯で鍵データが解読され、解読された鍵データとデータブロック毎に異なるシードからブロックキーが導かれることによりコンテンツの漏洩を引き起こす懸念が皆無とはいえない。

発明の開示

15 本発明は、上述の従来技術における問題点に鑑みてなされたものであり、DVD、CD等の各種情報記録媒体に格納したコンテンツを再生装置、PC（パーソナルコンピュータ）において利用する構成において、記録媒体に格納するコンテンツの暗号化に適用する鍵情報の漏洩をより困難とし、鍵解読、暗号アルゴリズムの解読の困難性を高めることを実現した情報処理装置、情報記録媒体ドライブ装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

20

本発明の第1の側面は、

25 情報記録媒体に格納された暗号化データの復号処理を実行する情報処理装置であり、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキー $Kb1$ を生成し、生成した第1ブロックキー $Kb1$ に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第

2シードに基づいて第2ブロックキーKb2を生成し、生成した第2ブロックキーKb2に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する暗号処理手段を有することを特徴とする情報処理装置にある。

5

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、マスターキー生成情報を格納した記憶手段を有し、前記暗号処理手段は、前記マスターキー生成情報に基づいてマスターキーを生成し、該生成したマスターキーと前記情報記録媒体からの読み出し情報とに基づいて、2つの記録キーK1, K2を生成し、生成した第1記録キーK1と前記第1シード情報とに基づく暗号処理により前記第1ブロックキーKb1を生成し、生成した第1ブロックキーKb1に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードと第2記録キーK2とに基づく暗号処理により前記第2ブロックキーKb2を生成し、生成した第2ブロックキーKb2に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する構成であることを特徴とする。

10

15

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクID、および前記情報記録媒体に記録された2つのタイトルキーに基づいて第1タイトル固有キーおよび第2タイトル固有キーを生成し、さらに、前記第1タイトル固有キーと、前記情報記録媒体からの第1読み出し情報とに基づく暗号処理により前記第1記録キーK1を生成し、前記第2タイトル固有キーと、前記情報記録媒体からの第2読み出し情報とに基づく暗号処理により前記第2記録キーK2を生成する構成であることを特徴とする。

20

25

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクID、および前記情報記録媒体に記録された1つのキーシード情報に基づいて第

- 1 タイトル固有キーおよび第2タイトル固有キーを生成し、さらに、前記第1
タイトル固有キーと、前記情報記録媒体からの第1読み出し情報とに基づく暗
号処理により前記第1記録キーK1を生成し、前記第2タイトル固有キーと、
前記情報記録媒体からの第2読み出し情報とに基づく暗号処理により前記第
5 2記録キーK2を生成する構成であることを特徴とする。

さらに、本発明の第2の側面は、

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行
する情報記録媒体ドライブ装置であり、

- 10 情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行
しセッションキーKsを生成する認証処理部と、

- 情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設
定された鍵生成情報としての第1シードに基づいて第1ブロックキーKb1
を生成し、生成した第1ブロックキーKb1に基づいて情報記録媒体に格納さ
15 れた暗号化第2シードの復号処理を実行して第2シードを取得し、前記セシ
ョンキーKsに基づいて前記第2シードを含むデータの暗号化処理を実行し
出力用暗号化情報を生成する暗号処理手段とを有し、

- 前記セッションキーKsに基づいて暗号化された第2シードを含む出力用
暗号化情報をインタフェースを介して出力する構成を有することを特徴とす
20 る情報記録媒体ドライブ装置にある。

- さらに、本発明の情報記録媒体ドライブ装置の一実施態様において、前記暗
号処理手段は、情報記録媒体ドライブ装置の保有するマスターキー生成情報に
基づいて生成したマスターキーと、前記情報記録媒体からの読み出し情報とに
25 基づいて、2つの記録キーK1、K2を生成し、生成した第1記録キーK1と
前記第1シード情報とに基づく暗号処理により前記第1ブロックキーKb1
を生成し、生成した第1ブロックキーKb1に基づいて情報記録媒体に格納さ
れた暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第
2シードと第2記録キーK2とを含むデータを前記セッションキーKsに基

づいて暗号化して出力用暗号化情報を生成し、前記第2シードと第2記録キーK2とを含む前記出力用暗号化情報をインタフェースを介して出力する構成を有することを特徴とする。

- 5 さらに、本発明の第3の側面は、
データ入力インタフェースを介して入力する暗号データの復号処理を実行する情報処理装置であり、
前記暗号データの出力装置との認証処理を実行しセッションキーKsを生成する認証処理部と、
- 10 前記データ入力インタフェースを介して入力する暗号化情報を前記セッションキーに基づく復号処理により鍵生成情報としてのシード情報および記録キーを取得し、前記シード情報および記録キーに基づく暗号処理により暗号データの復号キーとしてのブロックキーを生成し、該ブロックキーに基づく暗号データの復号処理を実行する暗号処理部と、
- 15 を有することを特徴とする情報処理装置にある。

さらに、本発明の第4の側面は、
情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報記録媒体ドライブ装置であり、

- 20 情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキーKsを生成する認証処理部と、
情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としてのシードに基づいてブロックキーを生成し、生成したブロックキーに基づいて情報記録媒体に格納された暗号化データの復号処理を実行して復号データを取得し、前記セッションキーKsに基づいて前記復号データの暗号化処理を実行し出力用暗号化情報を生成する暗号処理手段と
- 25 を有し、
前記セッションキーKsに基づいて暗号化された出力用暗号化情報をインタフェースを介して出力する構成を有することを特徴とする情報記録媒体ド

ライブ装置にある。

さらに、本発明の第 5 の側面は、
暗号化データを格納した情報記録媒体であり、

- 5 暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第 1 シードと、
前記第 1 シードに基づいて生成される第 1 ブロックキー $K_b 1$ に基づいて暗号化された鍵生成情報としての暗号化第 2 シードと、
前記第 2 シードに基づいて生成される第 2 ブロックキー $K_b 1$ に基づいて
- 10 暗号化された暗号化コンテンツと、
を格納した構成を有することを特徴とする情報記録媒体にある。

- さらに、本発明の情報記録媒体の一実施態様において、前記第 1 シードは、
前記暗号化処理単位毎に設定された制御情報内に格納され、前記第 2 シードは、
- 15 前記制御情報外のユーザデータ領域に暗号化されて格納された構成であることを特徴とする。

- さらに、本発明の情報記録媒体の一実施態様において、前記第 1 シードは、
ユーザデータ領域に非暗号化データとして格納され、前記第 2 シードは、ユー
- 20 ザデータ領域に暗号化データとして格納された構成であることを特徴とする。

- さらに、本発明の情報記録媒体の一実施態様において、前記暗号化データは、
トランスポートストリームパケットから構成され、前記第 1 シードは、複数の
トランスポートストリームパケットに対応する制御情報内に格納され、前記第
- 25 2 シードは、前記制御情報外のユーザデータ領域のトランスポートストリーム
パケット内に暗号化されて格納された構成であることを特徴とする。

さらに、本発明の情報記録媒体の一実施態様において、前記暗号化データは、
トランスポートストリームパケットから構成され、前記第 1 シードは、ユーザ

データ領域のトランスポートストリームパケット内に非暗号化データとして格納され、前記第2シードは、ユーザデータ領域のトランスポートストリームパケット内に暗号化されて格納された構成であることを特徴とする。

- 5 さらに、本発明の第6の側面は、
情報記録媒体に格納された暗号化データの復号処理を実行する情報処理方法であり、
情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキー K_b1
10 を生成するステップと、
生成した第1ブロックキー K_b1 に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードに基づいて第2ブロックキー K_b2 を生成するステップと、
生成した第2ブロックキー K_b2 に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップと、
15 を有することを特徴とする情報処理方法にある。

- さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、
さらに、記憶手段から読み出したマスターキー生成情報に基づいて生成したマ
20 スターキーと、前記情報記録媒体からの読み出し情報とに基づいて、2つの記録キー $K1$ 、 $K2$ を生成するステップを有し、生成した第1記録キー $K1$ と前記第1シード情報とに基づく暗号処理により前記第1ブロックキー K_b1 を生成し、生成した第1ブロックキー K_b1 に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2
25 シードと第2記録キー $K2$ とに基づく暗号処理により前記第2ブロックキー K_b2 を生成し、生成した第2ブロックキー K_b2 に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行することを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスク ID、および前記情報記録媒体に記録された 2 つのタイトルキーに基づいて第 1 タイトル固有キーおよび第 2 タイトル固有キーを生成し、さらに、前記第 1 タイトル固有キーと、前記情報記録媒体からの第 1 読み出し情報とに基づく暗号処理により前記第 1 記録キー K 1 を生成し、前記第 2 タイトル固有キーと、前記情報記録媒体からの第 2 読み出し情報とに基づく暗号処理により前記第 2 記録キー K 2 を生成するステップを有することを特徴とする。

10 さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスク ID、および前記情報記録媒体に記録された 1 つのキーシード情報に基づいて第 1 タイトル固有キーおよび第 2 タイトル固有キーを生成し、さらに、前記第 1 タイトル固有キーと、前記情報記録媒体からの第 1 読み出し情報とに基づく暗号処理により前記第 1 記録キー K 1 を生成し、前記第 2 タイトル固有キーと、前記情報記録媒体からの第 2 読み出し情報とに基づく暗号処理により前記第 2 記録キー K 2 を生成するステップを有することを特徴とする。

さらに、本発明の第 7 の側面は、

20 情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報処理方法であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキー K s を生成する認証処理ステップと、

25 情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第 1 シードに基づいて第 1 ブロックキー K b 1 を生成するステップと、

生成した第 1 ブロックキー K b 1 に基づいて情報記録媒体に格納された暗号化第 2 シードの復号処理を実行して第 2 シードを取得し、前記セッションキー K s に基づいて前記第 2 シードを含むデータの暗号化処理を実行し出力用

暗号化情報を生成するステップと、

前記セッションキー K_s に基づいて暗号化された第2シードを含む出力用暗号化情報をインタフェースを介して出力するステップと、
を有することを特徴とする情報処理方法にある。

5

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、
情報記録媒体ドライブ装置の保有するマスターキー生成情報に基づいて生成
したマスターキーと、前記情報記録媒体からの読み出し情報とに基づいて、2
つの記録キー K_1 、 K_2 を生成し、生成した第1記録キー K_1 と前記第1シード
10 情報とに基づく暗号処理により前記第1ブロックキー K_{b1} を生成し、生成
した第1ブロックキー K_{b1} に基づいて情報記録媒体に格納された暗号化第
2シードの復号処理を実行して第2シードを取得し、取得した第2シードと第
2記録キー K_2 とを含むデータを前記セッションキー K_s に基づいて暗号化
して出力用暗号化情報を生成し、前記第2シードと第2記録キー K_2 とを含む
15 前記出力用暗号化情報をインタフェースを介して出力することを特徴とする。

さらに、本発明の第8の側面は、

データ入力インタフェースを介して入力する暗号データの復号処理を実行
する情報処理方法であり、

20 前記暗号データの出力装置との認証処理を実行しセッションキー K_s を生成
する認証処理ステップと、

前記データ入力インタフェースを介して入力する暗号化情報を前記セッション
キーに基づく復号処理により鍵生成情報としてのシード情報および記録
キーを取得し、前記シード情報および記録キーに基づく暗号処理により暗号デ
25 ータの復号キーとしてのブロックキーを生成し、該ブロックキーに基づく暗号
データの復号処理を実行する暗号処理ステップと、
を有することを特徴とする情報処理方法にある。

さらに、本発明の第9の側面は、

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報処理方法であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキー K_s を生成する認証処理ステップと、

- 5 情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としてのシードに基づいてブロックキーを生成し、生成したブロックキーに基づいて情報記録媒体に格納された暗号化データの復号処理を実行して復号データを取得し、前記セッションキー K_s に基づいて前記復号データの暗号化処理を実行し出力用暗号化情報を生成する暗号処理ステップと、

- 10 プと、
前記セッションキー K_s に基づいて暗号化された出力用暗号化情報をインタフェースを介して出力するステップと、
を有することを特徴とする情報処理方法にある。

- 15 さらに、本発明の第10の側面は、

情報記録媒体に格納された暗号化データの復号処理を実行するコンピュータ・プログラムであり、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキー K_{b1}

- 20 を生成するステップと、

生成した第1ブロックキー K_{b1} に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードに基づいて第2ブロックキー K_{b2} を生成するステップと、

- 25 生成した第2ブロックキー K_{b2} に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップと、
を有することを特徴とするコンピュータ・プログラムにある。

本発明においては、本発明の構成によれば、暗号化コンテンツの復号に適用する鍵（ブロックキー K_{b2} ）を生成するために必要となるシード情報（シー

ド2)を他の鍵(ブロックキーKb1)によって暗号化して格納する構成としたので、シード情報(シード2)をディスクから直接読み取ることは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現さ

5 れる。

さらに、本発明の構成によれば、情報記録媒体に格納されたデータの再生処理において、暗号化コンテンツの復号に適用する鍵(ブロックキーKb2)生成用のシード情報(シード2)をデバイス間で転送することが必要となる構成
10 において、ブロックキー生成情報、具体的には、シード情報(シード2)および記録キーK2の双方をセッションキーで暗号化して送受信する構成としたので、転送路からのデータ漏洩が発生した場合であっても、シード情報(シード2)および記録キーK2を取得することは困難となり、シード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュ
15 リティレベルの高いコンテンツ保護が実現される。

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやDVD、MOなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピ
20 ュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

25 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

図面の簡単な説明

図 1 は、情報記録媒体に格納されるデータ構成について説明する図である。

図 2 は、情報処理装置の構成例について説明する図である。

5 図 3 は、情報処理装置において実行する復号処理について説明する図である。

図 4 は、ディスク固有キーの生成処理例について説明する図である。

図 5 は、記録キーの生成処理例について説明する図である。

図 6 は、記録キーを用いたデータ記録処理について説明する図である。

図 7 は、タイトル固有キーの生成処理例について説明する図である。

10 図 8 は、暗号化データの復号処理シーケンスを説明する図である。

図 9 は、暗号化データの復号処理シーケンスを説明する図である。

図 10 は、情報記録媒体に格納されるデータ構成について説明する図である。

図 11 は、情報処理装置において実行する復号処理について説明する図である。

15 図 12 は、暗号化データの復号処理シーケンスを説明する図である。

図 13 は、シード情報の格納構成例について説明する図である。

図 14 は、シード情報の格納構成例について説明する図である。

図 15 は、シード情報の格納構成例について説明する図である。

20 図 16 は、情報記録媒体ドライブ装置と情報処理装置間の接続構成を説明する図である。

図 17 は、情報記録媒体ドライブ装置と情報処理装置間のデータ転送処理を説明する図である。

図 18 は、情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う復号処理シーケンスを説明する図である。

25 図 19 は、情報記録媒体ドライブ装置と情報処理装置間の認証処理シーケンスを説明する図である。

図 20 は、情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う復号処理シーケンスを説明する図である。

図 21 は、情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う

復号処理シーケンスを説明する図である。

図 2 2 は、情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う復号処理シーケンスを説明する図である。

図 2 3 は、情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う

5 復号処理シーケンスを説明する図である。

発明を実施するための最良の形態

[記録媒体上のデータ記録構成]

10 まず、本発明に係る情報記録媒体に格納されたデータ構成について説明する。情報記録媒体に格納された暗号化データは、データ記録再生装置や、P C (パーソナルコンピュータ) において読み取られ、復号、再生される。

15 情報記録媒体に格納されるデータは、例えばMPEG-2システムで規定されている符号化データとしてのトランスポートストリーム(TS)である。トランスポートストリームは、1本のストリームの中に複数のプログラムを構成することができ、各トランスポートパケットの出現タイミング情報としてのA TS (Arrival Time Stamp: 着信時刻スタンプ) が設定されている。このタイムスタンプは、MPEG-2システムで規定されている仮想的なデコーダであ
20 るTSTD (Transport stream System Target Decoder)を破綻させないように符号化時に決定され、ストリームの再生時に、各トランスポートパケットに付加されたATSによって出現タイミングを制御して、復号、再生を行う。

25 例えば、トランスポートストリームパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。

図1を参照して、情報記録媒体に格納されるデータ記録構成および、記録データの復号再生処理の概要を説明する。情報記録媒体に格納されるデータは暗号化データであり、再生を行う場合には、復号処理を行うことが必要となる。

図1(a)が情報記録媒体に格納されるデータ記録構成である。18バイトの制御データ (User Control Data) と、2048バイトのユーザデータ (User Data) が1つのセクタデータとして構成され、例えば3セクタ分のデータが1つの暗号処理単位として規定される。なおここで説明するバイト数や、処理単位は1つの代表例であり、制御データ、ユーザデータのバイト数や、処理単位の設定は、様々な設定が可能である。

10

(b)は、暗号処理単位である1ユニット (1AU: Aligned Unit) の構成を示す。情報記録媒体に格納された暗号化データの再生を実行する情報処理装置は、制御データ内のフラグに基づいて、暗号処理単位である1AU (Aligned Unit) を抽出する。

15

暗号処理単位である1ユニット (1AU) には、(c) 暗号化構成に示すように、ブロックキーKb1によって暗号化された領域、ブロックキーKb2によって暗号化された領域が含まれる。ブロックキーKb1とKb2によって二重に暗号化された領域を含める構成としてもよい。ブロックキーを生成するためには、鍵生成情報としてのシード情報が必要となる。シード情報 (シード1) はブロックキーKb1を生成するための鍵生成情報であり、シード情報 (シード2) はブロックキーKb2を生成するための鍵生成情報である。これらは、制御データ領域、あるいはユーザデータ領域に格納される。図1(c)に示すシード情報の格納態様、暗号化態様は一例であり、後段において、複数の構成例について説明する。

25

ユーザデータ領域に格納された暗号化コンテンツを復号するためには、情報記録媒体に格納されたシード情報を読み取って、シード情報に基づく鍵を生成することが必要となる。

本発明の構成においては、図1(c)に示すように、ブロックキーKb1を生成するために必要となるシード情報(シード1)と、ブロックキーKb2を生成するために必要となるシード情報(シード2)とを情報記録媒体上に格納する構成とするとともに、一方のシード情報(シード2)をシード情報(シード1)によって生成されるブロックキーKb1によって暗号化して格納する構成とした。

このように、本発明の構成は、2つの異なる鍵を適用した暗号化処理を実行したデータを記録媒体に格納し、再生処理において2つの異なる鍵を適用した復号処理を行う。すなわち、所定の暗号処理単位毎に異なる鍵生成情報であるシード1、シード2を適用した暗号処理によりブロックキーKb1、Kb2を生成して復号処理を実行する。

1 処理単位毎の復号処理の後、復号されたトランスポートストリームパッケージがMPEG-2デコーダに入力されデコード処理が実行されてコンテンツ再生が行なわれる。1つの処理単位(3セクタ)には、例えば32個のトランスポートストリーム(TS)パッケージが含まれる。すなわち、 $32 \times 192 = 6144$ バイトデータが1つの暗号化および復号処理単位とされる。なお、処理単位の設定は、様々な設定が可能である。

復号再生時には、各処理単位毎に2つのシード情報(シード1、シード2)を情報記録媒体から取得し、各シード情報に基づいて2つのブロックキーKb1、Kb2を生成し、生成したブロックキーKb1、Kb2を用いて復号処理がなされて、コンテンツ再生が行われる。

また、コンテンツの記録時には、復号再生処理と逆のプロセスが実行され、各処理単位毎に2つのシード情報(シード1、シード2)を設定し、各シード情報に基づいて2つのブロックキーKb1、Kb2を生成し生成したブロック

キーK b 1, K b 2を用いて暗号化処理がなされて、コンテンツ記録が行われる。

[情報処理装置構成]

5 図2は、上述した暗号化コンテンツ態様を持つコンテンツの記録再生処理を実行する情報処理装置100の一実施例構成を示すブロック図である。情報処理装置100は、入出力I/F (Interface) 120、MPEG (Moving Picture Experts Group) コーデック130、A/D, D/Aコンバータ141を備えた入出力I/F (Interface) 140、暗号処理手段150、ROM (Read Only Memory) 160、CPU (Central Processing Unit) 170、メモリ180、
10 記録媒体195のドライブ190、さらにトランスポートストリーム処理手段(TS処理手段) 198を有し、これらはバス110によって相互に接続されている。

15 入出力I/F 120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F 140に出力するとともに、入出力I/F 140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F 140は、A/D, D/Aコンバータ141を内蔵している。入出力I/F 140は、外部から供給されるコンテンツとして
20 のアナログ信号を受信し、A/D, D/Aコンバータ141でA/D (Analog Digital)変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D, D/Aコンバータ141でD/A (Digital Analog)変換することで、アナログ信号として、外部に出力する。
25

暗号処理手段150は、例えば、1チップのLSI (Large Scale Integrated

Circuit)で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。暗号
5 処理手段150は、さらに、例えば入出力I/F120を介して接続された外部装置とのコンテンツ入出力の際に実行する認証処理を実行する認証処理部としても機能する。

ROM160は、例えば、情報処理装置ごとに固有の、あるいは、複数の情報
10 報処理装置のグループごとに固有のデバイスキーや、相互認証時に必要とする認証キーを記憶している。デバイスキーは、例えば鍵配信ツリー構成に基づいて提供される暗号化鍵ブロック情報としてのEKB (Enabling Key Block) を復号してマスターキーを取得するために用いられる。すなわち、デバイスキーは、マスターキー生成情報として適用される。

15 CPU170は、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータを記憶する。ドライブ190は、デジタルデータ
20 を記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し（再生し）、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。なお、プログラムをROM160に、マスターキー生成情報や認証キーをメモリ180に記憶するように構成してもよい。

25 記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはフラッシュROM、MRAM、RAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ190に対して着脱可能な構成であるとする。但し、記録媒体1

95は、情報処理装置100に内蔵する構成としてもよい。

5 トランスポートストリーム処理手段(TS処理手段)198は、複数のコンテンツが多重化されたトランスポートストリームから特定のコンテンツに対応するトランスポート packets を取り出して、取り出したトランスポートストリームの出現タイミング情報を各 packet とともに記録媒体195に格納するためのデータ処理を実行し、また、記録媒体195からの暗号化コンテンツの復号再生時には、トランスポートストリームの出現タイミング制御を行なう。

10 トランスポートストリームには、前述したように、各トランスポート packet の出現タイミング情報としてのATS (Arrival Time Stamp: 着信時刻スタンプ) が設定されており、MPEG2デコーダによる復号時にATSによってタイミング制御を実行する。トランスポートストリーム処理手段(TS処理手段)198は、例えば、トランスポート packet を記録媒体に記録する場合に
15 は、各 packet の間隔を詰めたソース packet として記録するが、各トランスポート packet の出現タイミングを併せて記録媒体に保存することにより、再生時に各 packet の出力タイミングを制御することが可能となる。

20 本発明の情報処理装置100は、例えば上述のトランスポートストリームによって構成される暗号化コンテンツの記録再生を実行する。これらの処理の詳細については、後段で説明する。なお、図2に示す暗号処理手段150、TS処理手段198は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する1つのワンチップLSIとして構成してもよく、また、両機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する
25 構成としてもよい。さらには、ドライブ190、記録媒体195を除く全てのブロックをワンチップLSIとして構成してもよく、また、これらの機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよく、これにより情報処理装置100の改造によるセキュリティ機能の無効化に対するロバストネスを向上させることが出来る。

[データ再生処理]

次に、記録媒体に格納された暗号化データの復号処理について説明する。図3にデータの復号処理の手順を説明する図を示す。図3に示す処理は、主に図2に示す暗号処理手段150が実行する処理である。

情報処理装置210は自身のメモリ180(図2参照)に格納しているマスターキー211を読み出す。マスターキー211は、ライセンスを受けた情報処理装置に格納された秘密キーであり、複数の情報処理装置に共通なキーとして格納された共通キーである。情報処理装置210は情報記録媒体220に識別情報としてのディスクID(Disc ID)221が既に記録されているかどうかを検査する。記録されていれば、ディスクID(Disc ID)221を情報記録媒体220から読出す。ディスクID(Disc ID)221は、ディスク固有情報であり、例えば一般データ格納領域または、リードインエリアに格納される。

次に、情報処理装置210は、ステップS101において、マスターキー211とディスクID221を用いて、ディスク固有キー(Disc Unique Key)を生成する。ディスク固有キー(Disc Unique Key)の具体的な生成方法としては、例えば、図4(a)に示すように、ディスクID(Disc ID)を入力値とし、共通鍵暗号方式であるAES(Advanced Encryption Standard)暗号を、マスターキー(Master Key)を暗号鍵として実行する方法や、図4(b)に示すように、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID(Disc ID)とのビット連結により生成されるデータを入力し、その出力から必要なデータ長のみをディスク固有キー(Disc Unique Key)として使用する方法が適用できる。

次に、記録コンテンツごとの2つの固有鍵であるタイトルキー(Title Key)1, 223、タイトルキー2, 224を情報記録媒体220から読出す。ディ

スク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーが格納されている。ディスク1枚に対してタイトルキーが1組しかない場合、すなわちディスクID221に対するタイトルキーが一意に決定できる場合には、ディスクID221と同様の方法で、例えば一般データ格納領域または、リードインエリアに格納するようにしてもよい。

次にステップS102およびステップS103において、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) 1, 2から、2つのタイトル固有キー (Title Unique Key) 1, 2を生成する。この生成の具体的な方法も、上記のように、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などが適用可能である。

さらに、情報処理装置210は、ステップS102およびステップS103において生成した2つのタイトル固有キー (Title Unique Key) 1, 2と、情報記録媒体220から読み出した記録シード (REC SEED) 225、物理インデックス226とに基づいて、ステップS104、S105において、2つの記録キー (RECキー) K1, K2を生成する。

ステップS102～S105において実行する2つの記録キー (RECキー) K1, K2の生成処理例について、図5を参照して説明する。

図5(a)は、図3のステップS102, S104の処理による記録キーK1の生成、図5(b)は、図3のステップS103, S105の処理による記録キーK2の生成処理例を示している。

図5(a)の処理は、まず情報記録媒体から読み出したタイトルキー1をAES (Advanced Encryption Standard) 暗号処理部271に入力し、ステップS101で生成したディスク固有キーを適用した復号処理 (Decryption) を実

行してタイトル固有キー 1 を生成 (S 1 0 2) して、さらに、情報記録媒体から読み出した物理インデックス 2 2 6 を A E S (Advanced Encryption Standard) 暗号処理部 2 7 2 に入力し、タイトル固有キー 1 を適用した暗号処理 (Encryption) を実行し、さらに、排他論理和部 2 7 3 において、暗号処理
5 結果とタイトル固有キー 1 の排他論理和演算を実行して、その出力を記録キー 1 として設定 (S 1 0 4) する処理である。

図 5 (b) の処理は、情報記録媒体から読み出したタイトルキー 2 を A E S (Advanced Encryption Standard) 暗号処理部 2 7 4 に入力し、ステップ S 1
10 0 1 で生成したディスク固有キーを適用した復号処理 (Decryption) を実行してタイトル固有キー 2 を生成 (S 1 0 3) して、さらに、情報記録媒体から読み出した記録シード (R E C S E E D) 2 2 5 を A E S (Advanced Encryption Standard) 暗号処理部 2 7 5 に入力し、タイトル固有キー 2 を適用した暗号処理 (Encryption) を実行して記録キー 2 を生成 (S 1 0 5) する
15 処理である。

記録キー K 1、K 2 は、上述の再生処理プロセスにおいて使用することが必要となるが、コンテンツを情報記録媒体に記録する暗号処理においても適用される鍵である。

20

図 6 に示すように、情報記録媒体 2 8 4 に格納される暗号化コンテンツは、まずコンテンツ編集スタジオ 2 8 2 において編集され、編集コンテンツがディスク製造工場等のディスク製造エンティティ 2 8 3 に渡されて、ディスク等の情報記録媒体に格納され、ユーザに提供される。

25

この製造プロセスにおいて、コンテンツ編集スタジオ 2 8 2 は、物理インデックスを設定するとともに、記録キー K 2 を適用した暗号化処理を編集コンテンツに対して実行し、ディスク製造エンティティ 2 8 3 は、記録シードを設定するとともに、記録キー K 1 を適用した暗号化処理を実行する。結果として情

報記録媒体 284 には、記録キー K1、K2 の 2 つの暗号鍵を用いた暗号処理が施された暗号化データが格納される。このようなディスク製造プロセスにおいて、コンテンツの管理を実行する管理センタ 281 が、コンテンツ編集スタジオには、タイトル固有キー 2 の取得可能情報を提供し、ディスク製造エンティティ 283 には、タイトル固有キー 1 の取得可能情報を提供する。

管理センタ 281 がこのような鍵管理を実行することで、管理センタ 281 からの鍵情報の提供を受けたコンテンツ編集スタジオ、およびディスク製造エンティティのみが、暗号化コンテンツの格納された情報記録媒体の製造が可能となり、不正な第三者による海賊版ディスクの製造が防止される。特に、コンテンツ編集スタジオが編集コンテンツに適用される TS パケット内に編集識別子（編集 ID）を格納して、これを編集コンテンツとともにコンテンツ編集スタジオで暗号化処理を施すことで、どの編集スタジオで加工された編集コンテンツであるかを秘匿したままディスク製造エンティティへデータを渡すことが可能となり、ディスク製造エンティティが受け入れるコンテンツの追跡管理が可能となる。

なお、図 3 に示す例では、2 つのタイトル固有キー 1, 2 を算出するために、情報記録媒体 220 に 2 つのタイトルキー 1, 2 を格納し、これらの 2 つのタイトルキーに基づいて、2 つのタイトル固有キーを算出する処理例を示したが、このように 2 つのタイトルキーを情報記録媒体 220 に格納することなく、1 つの格納情報のみから、2 つのタイトル固有キー 1, 2 を算出する構成も可能である。

図 7 を参照して 1 つの格納情報のみから、2 つのタイトル固有キー 1, 2 を算出する構成例を説明する。編集（オーサリング）毎に設定される乱数等のランダム値をディスクキーシードとして情報記録媒体 220 に格納する。

図 7 (a) の処理例は、ディスクキーシードに対してディスク固有キーを適

用して、AES暗号処理部291において暗号処理を実行し、その出力をタイトル固有キー1とする。さらにそのタイトル固有キー1をAES暗号処理部292に入力しディスク固有キーを適用してAES暗号処理を実行し、その結果をタイトル固有キー2とする。

5

図7(b)の処理例は、ディスクキーシードに対してディスク固有キーを適用して、AES暗号処理部293において暗号処理を実行し、その出力をタイトル固有キー1とする。さらにそのタイトル固有キー1を、演算部294において、演算、例えば、 $(\text{ディスクキーシード} + 1) \bmod 2^{128}$ を算出し、その結果をAES暗号処理部295に入力しディスク固有キーを適用してAES暗号処理を実行し、その結果をタイトル固有キー2とする。図7に示す方法によれば、情報記録媒体220に格納する情報を少なくすることが可能となる。

10

図3に戻り、情報記録媒体からのデータ復号、再生処理についての説明を続ける。ステップS104、S105において2つの記録キー(RECキー)1, 2を生成すると、次に、ステップS106において、ブロックキーKb1の生成処理を実行する。

15

ブロックキーKb1の生成処理においては、情報記録媒体220からブロックキーKb1生成情報としてのシード情報(シード1)227を読み出し、シード情報(シード1)227と、ステップS104において生成した記録キーK1とに基づく暗号処理を実行してブロックキーKb1を生成する。

20

ステップS106のブロックキーKb1の生成処理以降に実行する処理について、図8を参照して説明する。

25

図8において、復号処理は、処理単位300を単位として実行される。この処理単位は、先に図1を参照して説明した(b)処理単位に相当する。すなわち、暗号処理単位である1ユニット(1AU: Aligned Unit)である。情報記

録媒体 220 に格納された暗号化データの再生を実行する情報処理装置 210 は、制御データ内のフラグに基づいて、暗号処理単位である 1 AU (Aligned Unit) を抽出する。

- 5 処理単位 300 には、18 バイトの制御データ 301 と、6144 バイトのユーザデータ (暗号化コンテンツを含む) が含まれる。6144 バイトのユーザデータは、トランスポートストリームパケットの単位である 192 バイト毎に分割される。ユーザデータの先頭の TS パケット 302 と、後続の 5952 バイトの TS パケット群 303 を分離して説明する。この例では、シード情報
- 10 (シード 1) 311 が制御データ 301 に格納され、シード情報 (シード 2) 312 がユーザデータ内の先頭の TS パケット 302 内に暗号化されて格納された例である。

- 15 なお、シード情報としての、シード 1、シード 2 の格納態様には複数の態様があり、ここではその一例を示す。他の例については、後段で説明する。

図 8 において、図 3 の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

- 20 ステップ S106 (図 3、図 8) においては、情報記録媒体の制御データ内から読み出したシード情報 (シード 1) 311 を AES 暗号処理部に入力し、先のステップ S104 において生成した記録キー K1 を適用した AES 暗号処理を実行しブロックキー Kb1 を生成する処理を実行する。なお、図 8 において AES_G は、AES 暗号処理を適用した鍵生成 (Key Generation) 処理
- 25 を示し、AES_D は、AES 暗号処理を適用したデータ復号 (Decryption) 処理を示している。

次に、図 3 のステップ S107 において、32 TS パケットからなるユーザデータから暗号化データ部のみが抽出される。ユーザデータの暗号化部、非暗

号化部がステップS107において分離されて、暗号化部のみがステップS108～S111の復号処理プロセス対象とされる。非暗号化部は、ステップS108～S111をスキップし、ステップS112において、再度セレクトステップにより復号データと連結され、復号TS packets群として、例えばMP
5 EGデコーダに入力され、デコード処理がなされる。

ステップS108（図3、図8参照）では、ステップS106において生成したブロックキーKb1を適用したAES復号処理を実行する。ステップS108では、ブロックキーKb1を適用した暗号処理のなされたデータ部のみを
10 対象とした復号処理が実行される。この例では、ユーザデータの先頭TS packets302の少なくともシード情報（シード2）を含むデータ領域がブロックキーKb1を適用した暗号処理のなされたデータ部である。従って、このシード情報（シード2）を含むデータ領域を対象としてブロックキーKb1を適用した復号処理を実行する。

15

なお、ブロックキーKb1を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては後述する。

20 先頭TS packets302には、他のユーザデータ部、すなわち、後続の5952バイトのTS packets群303の復号処理に適用するブロックキーKb2を算出するために必要となるシード情報（シード2）312が含まれている。すなわち、シード情報（シード2）312は、ブロックキーKb1を適用した暗号処理がなされた暗号化データとして先頭TS packets302に記録され
25 ている。

ステップS106における、ブロックキーKb1を適用した復号処理の結果として、復号TS packets304が算出され、その中からシード情報（シード2）を抽出する。

図3のセレクトステップS109は、ブロックキーKb1を適用した復号処理の結果から、シード情報（シード2）をステップS110のブロックキーKb2生成ステップに出力し、ブロックキーKb2で暗号化された暗号化データを復号ステップS111に出力し、その他の復号データ（非暗号化データ）をセレクトステップS112に出力することを示している。

ステップS110（図3，図8参照）では、ステップS108におけるブロックキーKb1を適用した復号処理の結果取得された復号TSパケット304から抽出したシード情報（シード2）と、ステップS105（図3参照）において生成した記録キーK2とに基づいて、AES暗号処理を実行し、ブロックキーKb2を算出する。

次に、ステップS111において、ブロックキーKb2を適用してユーザデータ部の暗号化部（ブロックキーKb2で暗号化されたデータ領域303）を復号し、復号TSパケット群305を生成する。

復号TSパケット群305、および復号TSパケット304は、セレクトステップS112において結合されて、復号TSパケットとして例えばMPEG2デコーダに入力され、デコードされた後、再生される。

このように、本発明の構成においては、暗号化コンテンツの復号に適用する鍵（ブロックキーKb2）を生成するために必要となるシード情報（シード2）を他の鍵（ブロックキーKb1）によって暗号化して格納する構成としたので、シード情報（シード2）をディスクから直接読み取ることは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

なお、2つのシード情報の格納形態には、様々な態様があり、以下、複数の

例について説明する。

図 9 に、シード情報（シード 1）と、シード情報（シード 2）とを共にユーザデータ内の先頭 TS パケット 3 0 2 内に格納した例を示す。先に図 8 を参照して説明した例では、シード情報（シード 1）3 1 1 が制御データ 3 0 1 に格納され、シード情報（シード 2）3 1 2 がユーザデータ内の先頭の TS パケット 3 0 2 内に暗号化されて格納された例を説明したが、図 9 に示す構成例は、シード情報（シード 1）3 2 1、シード情報（シード 2）3 2 2、双方がユーザデータ内の先頭の TS パケット 3 0 2 内に格納された例である。

10

なお、シード情報（シード 2）3 2 2 は、図 8 において説明した例と同様、シード情報（シード 1）3 2 1 を適用して取得されるブロックキー Kb 1 によって暗号化されてユーザデータ内の先頭の TS パケット 3 0 2 内に格納される。

15

図 9 において、復号処理は、処理単位 3 0 0 を単位として実行される。この処理単位は、先に図 1 を参照して説明した（b）処理単位に相当する 1 ユニット（1 AU : Aligned Unit）である。情報記録媒体 2 2 0 に格納された暗号化データの再生を実行する情報処理装置 2 1 0 は、制御データ内のフラグに基づいて、暗号処理単位である 1 AU（Aligned Unit）を抽出する。

20

あるいは、暗号化処理単位ごとに暗号化が施されたユニットであるか暗号化が施されていないユニットであるかを判別するため、暗号化処理単位の先頭に存在するシード情報 3 2 1 に含まれるフラグを利用する厚生とすることができ。シード情報を含めた暗号化処理単位の先頭部分を表した例が図 1 0 である。図 1 0 のコピー制御情報としての CCI 部分に記録されたフラグを利用して暗号化の有無を判別することができる。暗号化されている場合は復号化を行う経路を通し再生を行う。暗号化されていない場合は復号化を行う経路を通さずに再生を行う。

25

図 11 に、CCI 部分に記録されたフラグを利用して暗号化の有無を判別し、暗号化されている場合は復号化を行う経路を通し再生を行い、暗号化されていない場合は復号化を行う経路を通さずに再生を行う処理を実行する場合の処理構成を示す。図 11 において、先の図 3 に示す構成との違いは、セレクトステップ S 107 が、シード情報（シード 1）227 を入力し、シード情報（シード 1）227 の CCI 部分に記録されたフラグを利用して暗号化の有無を判別し、暗号化されている場合は復号化を行う経路を通し、暗号化されていない場合は復号化を行う経路を通さずに再生を行う選択処理を実行する点のみである。他の処理は、図 3 に示す処理と同様である。

図 9 の処理について説明する。図 9 において、図 11 の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

ステップ S 106（図 11、図 9）は、情報記録媒体のユーザデータの先頭 TS パケット内から読み出したシード情報（シード 1）321 を AES 暗号処理部に入力し、先のステップ S 104（図 11 参照）において生成した記録キー K1 を適用した AES 暗号処理を実行しブロックキー Kb1 生成処理を実行するステップである。

次に、図 11 のステップ S 107 において、32 TS パケットからなるユーザデータから暗号化データ部のみが抽出される。ユーザデータの暗号化部、非暗号化部がステップ S 107 において分離されて、暗号化部のみがステップ S 108～S 111 の復号処理プロセス対象とされる。非暗号化部は、ステップ S 108～S 111 をスキップし、ステップ S 112 において、再度セレクトステップにより復号データと連結され、復号 TS パケット群として、例えば MPEG デコーダに入力され、デコード処理がなされる。

ステップ S 108（図 11、図 9 参照）では、ステップ S 106 において生

成したブロックキーK b 1を適用したAES復号処理が実行される。ステップS 1 0 8では、ブロックキーK b 1を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭TSパケット3 0 2中、少なくともシード情報(シード2) 3 2 2を含むデータ領域の復号処理が実行される。

この先頭TSパケット3 0 2の暗号化データ領域には、他のユーザデータ部、すなわち、後続の5 9 5 2バイトのTSパケット群3 0 3の復号処理に適用するブロックキーK b 2を算出するために必要となるシード情報(シード2) 3 2 2が含まれている。すなわち、シード情報(シード2) 3 2 2は、ブロックキーK b 1を適用した暗号処理がなされた暗号化データとして先頭TSパケット3 0 2に記録されている。

ステップS 1 0 6における、ブロックキーK b 1を適用した復号処理の結果として、復号TSパケット3 0 4が算出され、その中からシード情報(シード2)を抽出する。

図3のセレクトステップS 1 0 9は、ブロックキーK b 1を適用した復号処理の結果から、シード情報(シード2)をステップS 1 1 0のブロックキーK b 2生成ステップに出力し、ブロックキーK b 2で暗号化された暗号化データを復号ステップS 1 1 1に出力し、その他の復号データ(非暗号化データ)をセレクトステップS 1 1 2に出力することを示している。

ステップS 1 1 0(図11, 図9参照)では、ステップS 1 0 8におけるブロックキーK b 1を適用した復号処理の結果取得された復号TSパケット3 0 4から抽出したシード情報(シード2)と、ステップS 1 0 5(図11参照)において生成した記録キーK 2とに基づいて、AES暗号処理を実行し、ブロックキーK b 2を算出する。

次に、ステップS111において、ブロックキーKb2を適用してユーザデータ部の暗号化部（ブロックキーKb2で暗号化されたデータ領域303）を復号し、復号TSパケット群305を生成する。

- 5 復号TSパケット群305、および復号TSパケット304は、セレクトステップS112において結合されて、復号TSパケットとして例えばMP EG 2デコーダに入力され、デコードされた後、再生される。

10 このように、本構成においては、シード情報（シード1）と、シード情報（シード2）とを共にユーザデータ内の先頭TSパケット内に格納し、ブロックキーKb2を生成するために必要となるシード情報（シード2）は、シード情報（シード1）と、記録キーK1とに基づいて生成するブロックキーKb1によって暗号化して格納する構成とした。

- 15 本構成においても、シード情報（シード2）をディスクから直接読み取ることとは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

- 20 図12に示す例は、シード情報（シード1）331をユーザデータ内の先頭TSパケット302に格納し、シード情報（シード2）332をユーザデータ内の次のTSパケット341に格納した例である。

- 25 なお、シード情報（シード2）332は、図8、図9において説明した例と同様、シード情報（シード1）331を適用して取得されるブロックキーKb1によって暗号化されてユーザデータ内の第2のTSパケット341内に格納される。

図12において、復号処理は、処理単位300を単位として実行される。こ

の処理単位は、先に図 1 を参照して説明した (b) 処理単位に相当する 1 ユニ
ット (1 AU: Aligned Unit) である。情報記録媒体 220 に格納された暗号
化データの再生を実行する情報処理装置 210 は、制御データ内のフラグに基
づいて、暗号処理単位である 1 AU (Aligned Unit) を抽出する。

5

あるいは、暗号化処理単位ごとに暗号化が施されたユニットであるか暗号化
が施されていないユニットであるかを判別するため、暗号化処理単位の先頭に
存在するシード情報 321 に含まれるフラグを利用する。シード情報を含めた
暗号化処理単位の先頭部分を表した例が図 10 である。図 10 の CCI 部分に
10 記録されたフラグを利用して暗号化の有無を判別することができる。暗号化さ
れている場合は復号化を行う経路を通し再生を行う。暗号化されていない場合
は復号化を行う経路を通さずに再生を行う。

図 12 の処理について説明する。図 12 において、図 3 の処理ステップと同
15 様の処理ステップには、同一の処理ステップ番号を付してある。

ステップ S106 (図 1.1、図 1.2) は、情報記録媒体のユーザデータの先
頭 TS パケット内から読み出したシード情報 (シード 1) 331 を AES 暗号
処理部に入力し、先のステップ S104 (図 1.1 参照) において生成した記録
20 キー K1 を適用した AES 暗号処理を実行してブロックキー Kb1 を生成す
るステップである。

次に、図 3 のステップ S107 において、32 TS パケットからなるユーザ
データから暗号化データ部のみが抽出される。ユーザデータの暗号化部、非暗
25 号化部がステップ S107 において分離されて、暗号化部のみがステップ S1
08 ~ S111 の復号処理プロセス対象とされる。非暗号化部は、ステップ S
108 ~ S111 をスキップし、ステップ S112 において、再度セレクトス
テップにより復号データと連結され、復号 TS パケット群として、例えば MP
EG デコーダに入力され、デコード処理がなされる。

ステップS108（図11、図12参照）では、ステップS106において生成したブロックキーKb1を適用したAES復号処理を実行する。復号処理対象は、ブロックキーKb1を適用した暗号処理がなされているデータ領域で
5 あり、ユーザデータの先頭TSパケット中のシード情報（シード1）321を除くデータ領域の暗号化領域と、第2TSパケット中の少なくともシード情報（シード2）332を含むデータ領域の復号処理が実行される。ブロックキーKb1を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては後述する。

10 本例では、第2のTSパケット341の暗号化データ領域に、他のユーザデータ部、すなわち、後続のTSパケット群342の復号処理に適用するブロックキーKb2を算出するために必要となるシード情報（シード2）332が含まれる。すなわち、シード情報（シード2）332は、ブロックキーKb1を
15 適用した暗号処理がなされた暗号化データとして第2TSパケット341に記録されている。

ステップS106における、ブロックキーKb1を適用した復号処理の結果として、復号TSパケット304が算出され、その中からシード情報（シード
20 2）を抽出する。

図11のセクタステップS109は、ブロックキーKb1を適用した復号処理の結果から、シード情報（シード2）をステップS110のブロックキーKb2生成ステップに出力し、ブロックキーKb2で暗号化された暗号化データ
25 を復号ステップS111に出力し、その他の復号データ（非暗号化データ）をセクタステップS112に出力することを示している。

ステップS110（図11、図12参照）では、ステップS108におけるブロックキーKb1を適用した復号処理の結果、取得された復号TSパケット

304から抽出したシード情報(シード2)と、ステップS105(図11参照)において生成した記録キーK2とに基づいて、AES暗号処理を実行し、ブロックキーKb2を算出する。

- 5 次に、ステップS111において、ブロックキーKb2を適用してユーザデータ部の暗号化部(ブロックキーKb2で暗号化されたデータ領域342)を復号し、復号TSパケット群305を生成する。

- 10 復号TSパケット群305、および復号TSパケット304は、セレクトステップS112において結合されて、復号TSパケットとして例えばMP EG2デコーダに入力され、デコードされた後、再生される。

- 15 このように、本構成においては、シード情報(シード1)ユーザデータ内の先頭TSパケット内に格納し、ブロックキーKb2を生成するために必要となるシード情報(シード2)をユーザデータ内の第2TSパケット内に格納し、シード情報(シード2)を、シード情報(シード1)と、記録キーK1とに基づいて生成するブロックキーKb1によって暗号化して格納する構成とした。

- 20 本構成においても、シード情報(シード2)をディスクから直接読み取ることは不可能である。従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

- 25 次に、図13、図14、図15を参照してシード情報(シード1)と記録キーKに基づいて生成するブロックキーKb1によって暗号化する領域の例について説明する。図13は、制御ブロックにシード情報(シード1)が格納され、シード情報(シード2)が、ユーザデータの1つのTSパケットに含まれる場合の例である。図8、図9、図12を参照して説明した例では、シード情報(シード2)が、ユーザデータの先頭または2番目のTSパケット内に含ま

れる場合について説明したが、シード情報（シード2）は、先頭、または第2番目のTSパケット以外のユーザデータ部を構成する任意のTSパケット内に格納可能である。

- 5 ユーザデータのいずれかのTSパケットにシード情報（シード2）を格納した場合、シード情報（シード1）と記録キーK1とに基づいて生成するブロックキーKb1によって暗号化する領域例として、例えば図13（a）～（c）の構成がある。（a）は、シード情報（シード2）のみをブロックキーKb1によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あ
- 10 るいは、シード情報（シード2）と記録キーK2によって生成されるブロックキーKb2によって暗号化したデータ領域とする。

（b）は、シード情報（シード2）を含むTSパケットの一部領域をブロックキーKb1によって暗号化した例である。

15

コンテンツ編集スタジオ282（図6参照）においてシード情報（シード2）と編集識別子（編集ID）をTSパケット内に格納し、ディスク製造エンティティ283（図6参照）において、シード情報（シード1）に基づいて生成可能な記録キーK1を用いて、シード情報（シード2）の暗号化処理を行った後、

- 20 ディスクに格納する。

（c）は、シード情報（シード2）を含む1つのTSパケットの全領域をブロックキーKb1によって暗号化した例である。

- 25 図14に示す例は、シード情報（シード1）とシード情報（シード2）を同一のTSパケット内に格納した例を示している。シード情報（シード1）は非暗号化情報として格納される。シード情報（シード2）は、シード情報（シード1）と記録キーK1とに基づいて生成するブロックキーKb1によって暗号化され、シード情報（シード1）と同一のTSパケット内に格納される。

(d) は、シード情報 (シード 2) のみをブロックキー K b 1 によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報 (シード 2) と記録キー K 2 によって生成されるブロックキー K b 2 によって暗号化したデータ領域とする。

(e) は、シード情報 (シード 2) を含む TS パケットの一部領域をブロックキー K b 1 によって暗号化した例である。(f) は、シード情報 (シード 2) を含む 1 つの TS パケットの全領域をブロックキー K b 1 によって暗号化した例である。

図 1 5 に示す例は、シード情報 (シード 1) とシード情報 (シード 2) を異なる TS パケット内に格納した例を示している。シード情報 (シード 1) は非暗号化情報として格納される。シード情報 (シード 2) は、シード情報 (シード 1) と記録キー K 1 とに基づいて生成するブロックキー K b 1 によって暗号化され、シード情報 (シード 1) と異なる TS パケット内に格納される。

(g) は、シード情報 (シード 2) のみをブロックキー K b 1 によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報 (シード 2) と記録キー K 2 によって生成されるブロックキー K b 2 によって暗号化したデータ領域とする。

(h) は、シード情報 (シード 2) を含む TS パケットの一部領域をブロックキー K b 1 によって暗号化した例である。(i) は、シード情報 (シード 2) を含む 1 つの TS パケットの全領域をブロックキー K b 1 によって暗号化した例である。

以上、図 1 3 ~ 図 1 5 を参照して説明したように、シード情報 (シード 1) およびシード情報 (シード 2) の格納態様、および暗号化データ領域の設定態

- 様は様々な設定が可能である。しかし、いずれの場合もシード情報（シード2）は、シード情報（シード1）を用いて生成される鍵、すなわちブロックキーKb1によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード2）の解析、シード情報（シード2）を適用して生成するブロックキーKb2の解析、ブロックキーKb2によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

10 成]

[情報記録媒体ドライブ装置とのインタフェースを介するデータ入出力構

次に、P.C等の情報処理装置において、様々なインタフェース、例えばSCSI、IEEE1394、USB等のインタフェースを介してDVD、CD等の情報記録媒体を装着した情報記録媒体ドライブと接続し、インタフェースを介してデータ転送を実行する場合の処理例について説明する。

15

例えば、図15に示すように、P.C等の情報処理装置410と、DVD、CD等の情報記録媒体430を装着した情報記録媒体ドライブ420とを双方のインタフェース411、421を介して接続した構成であり、情報記録媒体ドライブ420が情報記録媒体430に対するアクセスを実行し、データを双方のインタフェース411、421を介して転送し、P.C等の情報処理装置410において再生する構成である。

20

図に示すように、インタフェース411、421を介してデータが転送される場合、転送データに上述したシード情報（シード2）が非暗号化状態で含まれると、転送データからのシード情報（シード2）の漏洩が発生する可能性がある。

25

そこで、本発明の構成においては、情報処理装置410と情報記録媒体ドライブ420間でインタフェースを介してデータ転送が実行される場合、双方の

装置間において、認証処理を実行し、認証処理の結果、双方の機器で取得するセッションキーを用いて転送データを暗号化して送信する構成とした。以下、この処理構成の詳細について説明する。

5 図17に、PC等の情報処理装置500と情報記録媒体ドライブ510において、暗号化コンテンツを格納した情報記録媒体520のデータ読み出し、再生を実行する場合の処理を説明する図を示す。なお、情報処理装置500と情報記録媒体ドライブ510とも、先に図2を参照して説明した構成とほぼ同様の構成を持つ。ただし、PC等の情報処理装置500は、図2に示す記録媒体
10 195およびドライブ190は必須ではなく、これらは、情報記録媒体ドライブ510のみが備えていればよい。また、MPEGコーデック130、TS処理手段198はPC等の情報処理装置500のみが有する構成でよく、情報記録媒体ドライブ510には構成する必要がない。

15 図17を参照して、情報記録媒体520のデータを情報記録媒体ドライブ510において読み出し、情報処理装置500に転送して再生する場合の処理を説明する。

情報記録媒体ドライブ510は自身のメモリ180（図2参照）に格納しているマスターキー511を読み出す。なお、マスターキー511は、情報処理
20 装置500側に格納されている場合は、情報処理装置500から情報記録媒体ドライブ510に送信してもよい。マスターキー511は、ライセンスを受けた情報処理装置（情報記録媒体ドライブを含む）に格納された秘密キーであり、複数の情報処理装置に共通なキーとして格納された共通キーである。

25 情報記録媒体ドライブ510は、ディスクID（Disc ID）521を情報記録媒体520から読出す。ディスクID（Disc ID）521は、ディスク固有情報であり、例えば一般データ格納領域または、リードインエリアに格納される。

次に、情報記録媒体ドライブ 5 1 0 は、ステップ S 5 5 1 において、マスターキー 5 1 1 とディスク ID 5 2 1 を用いて、ディスク固有キー (Disc Unique Key) を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法は、先に図 4 を参照して説明したと同様の方法が適用できる。

次に、記録コンテンツごとの 2 つの固有鍵であるタイトルキー (Title Key) 1, 5 2 3、タイトルキー 2, 5 2 4 を情報記録媒体 5 2 0 から読出す。ディスク上には、どこかのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーが格納されている。ディスク 1 枚に対してタイトルキーが 1 組しかない場合、すなわちディスク ID 5 2 1 に対するタイトルキーが一意に決定できる場合には、ディスク ID 5 2 1 と同様の方法で、例えば一般データ格納領域または、リードインエリアに格納するようにしてもよい。

15

次にステップ S 5 5 2 およびステップ S 5 5 3 において、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) 1, 2 から、2 つのタイトル固有キー (Title Unique Key) 1, 2 を生成する。

20

さらに、情報記録媒体ドライブ 5 1 0 は、ステップ S 5 5 2 およびステップ S 5 5 3 において生成した 2 つのタイトル固有キー (Title Unique Key) 1, 2 と、情報記録媒体 5 2 0 から読み出した記録シード (REC SEED) 5 2 5、物理インデックス 5 2 6 とに基づいて、ステップ S 5 5 4、S 5 5 5 において、2 つの記録キー (REC キー) K 1, K 2 を生成する。

25

ステップ S 5 5 2 ~ S 5 5 5 において実行する 2 つの記録キー (REC キー) K 1, K 2 の生成処理は、先に図 5 を参照して説明した通り、2 つのタイトル固有キー (Title Unique Key) 1, 2 と、情報記録媒体 5 2 0 から読み出した記録シード (REC SEED) 5 2 5、物理インデックス 5 2 6 とに基づ

づくAES (Advanced Encryption Standard) 暗号処理により生成される。

5 なお、先に図7を参照して説明した通り、記録シード (REC SEED)
525、物理インデックス526を情報記録媒体520に格納する代わりに編
集 (オーサリング) 毎に設定される乱数等のランダム値をディスクキーシード
として情報記録媒体520に格納して、ディスクキーシードに対してディスク
固有キーを適用して、AES暗号処理を実行し、その出力からタイトル固有キ
ー1、タイトル固有キー2を得る方法としてもよい。

10 上述のいずれかの方法により、ステップS554、S555において2つの
記録キー (RECキー) 1, 2を生成すると、次に、ステップS556におい
て、ブロックキーKb1の生成処理を実行する。

15 ブロックキーKb1の生成処理においては、情報記録媒体520からブロッ
クキーKb1生成情報としてのシード情報 (シード1) 527を読み出し、シ
ード情報 (シード1) 527と、ステップS554において生成した記録キー
K1とに基づく暗号処理を実行してブロックキーKb1を生成する。

20 ステップS556のブロックキーKb1の生成処理以降に実行する処理に
ついて、図18を参照して説明する。

図18において、復号処理は、図8～図12を参照して説明したと同様、処
理単位600を単位として実行される。この処理単位は、先に図1を参照して
説明した (b) 処理単位に相当する。すなわち、暗号処理単位である1ユニッ
25 ト (1AU: Aligned Unit) である。情報記録媒体520に格納された暗号化
データの読み取りを実行する情報記録媒体ドライブ510は、制御データ内の
フラグに基づいて、暗号処理単位である1AU (Aligned Unit) を抽出する。

処理単位600には、18バイトの制御データ601と、6144バイトの

ユーザデータ（暗号化コンテンツを含む）が含まれる。6144バイトのユーザデータは、トランスポートストリームパケットの単位である192バイト毎に分割される。ユーザデータの先頭のTSパケット602と、後続の5952バイトのTSパケット群603を分離して説明する。この例では、シード情報

5 （シード1）611が制御データ601に格納され、シード情報（シード2）612がユーザデータ内の先頭のTSパケット602内に暗号化されて格納された例である。

10 なお、シード情報としての、シード1、シード2の格納態様には複数の態様があり、ここではその一例を示す。他の例については、後段で説明する。

図18において、図17の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

15 ステップS556（図17、図18）は、情報記録媒体の制御データ内から読み出したシード情報（シード1）611をAES暗号処理部に入力し、先のステップS554において生成した記録キーK1を適用したAES暗号処理を実行しブロックキーKb1生成処理を実行するステップである。

20 次に、図17のステップS557において、32TSパケットからなるユーザデータからブロックキーKb1による暗号化データ部のみが抽出される。ブロックキーKb1による暗号化データ部、非暗号化部がステップS557において分離されて、暗号化部のみがステップS558において復号される。非暗号化部は、ステップS558をスキップし、ステップS559において、再度

25 セレクトステップにより復号データと連結され、ステップS563においてセッションキーによって暗号化がなされる。

ステップS558（図17、図18参照）では、ステップS556において生成したブロックキーKb1を適用したAES復号処理を実行する。ステップ

S 5 5 8では、ブロックキーK b 1を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭TS
5 パケット6 0 2の少なくともシード情報(シード2)を含むデータ領域がブロックキーK b 1を適用した暗号処理のなされたデータ部である。従って、このシード情報(シード2)を含むデータ領域を対象としてブロックキーK b 1を適用した復号処理を実行する。

10 なお、ブロックキーK b 1を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては、先に、図1 3～図1 5を参照して説明した通りである。

15 先頭TSパケット6 0 2には、他のユーザデータ部、すなわち、後続の5 9 5 2バイトのTSパケット群6 0 3の復号処理に適用するブロックキーK b 2を算出するために必要となるシード情報(シード2)6 1 2が含まれている。すなわち、シード情報(シード2)6 1 2は、ブロックキーK b 1を適用した暗号処理がなされた暗号化データとして先頭TSパケット6 0 2に記録されている。

20 ステップS 5 5 6における、ブロックキーK b 1を適用した復号処理の結果として、復号TSパケット6 0 4が算出され、その中には、シード情報(シード2)が含まれる。

25 図1 7のセレクトステップS 5 5 9は、ブロックキーK b 1を適用した復号処理の結果から、シード情報(シード2)を含む復号データと、その他のデータを結合して、暗号化ステップS 5 6 3に出力することを示している。

ステップS 5 6 3における暗号化処理は、情報記録媒体ドライブ5 1 0と、情報処理装置5 0 0との間で実行する相互認証処理の結果として双方で共有するセッションキーに基づいて実行する暗号処理である。相互認証処理は、情

情報記録媒体ドライブ510と、情報処理装置500とが共有する認証キー K_m 530, 540に基づいて実行される。

5 相互認証処理のシーケンスについて、図19を参照して説明する。図19に示す認証およびセッションキー共有処理は、共通鍵処理方式に基づく一例である。認証シーケンスおよびセッションキー共有シーケンスは、この処理シーケンスに限らず、他の処理方法を適用してもよい。

10 情報記録媒体ドライブ510と、情報処理装置500は認証キー K_m 530, 540を有する。まず、ステップS571において、情報処理装置500が乱数 R_{b1} (64 bit) を生成し、情報記録媒体ドライブ510に送信する。情報記録媒体ドライブ510は、ステップS581において、乱数 R_{a1} を生成し、ステップS682において、乱数 R_{a1} と乱数 R_{b1} の結合データ $[R_{a1} \parallel R_{b1}]$ に対するAES暗号化処理に基づくMAC (Message Authentication Code) を生成する。生成MAC値を $e_{K_m}(R_{a1} \parallel R_{b1})$ とする。なお、 $e_{K_a}(B)$ は、キー K_a によるデータ B の暗号化を示し、 $A \parallel B$ は、データ A とデータ B の連結を示す。情報記録媒体ドライブ510は、生成MAC値: $e_{K_m}(R_{a1} \parallel R_{b1})$ と、生成乱数 R_{a1} を情報処理装置500に送信する。

20 情報処理装置500は、情報記録媒体ドライブ510から受信した乱数 R_{a1} とステップS571において生成した乱数 R_{b1} とに基づいて、ステップS572において、MAC値: $e_{K_m}(R_{a1} \parallel R_{b1})$ を算出する。さらに、ステップS573において、算出したMAC値と、情報記録媒体ドライブ510から受信したMAC値とを比較する。一致すれば、情報処理装置500は、情報記録媒体ドライブ510が正しい認証キーを持つ正規なデバイスであると認証する。不一致の場合は、認証エラーであり、その後の処理を中止する。

さらに、情報処理装置500は、ステップS574において、乱数 R_{b2} を

生成し、情報記録媒体ドライブ510に送信する。情報記録媒体ドライブ510は、ステップS583において、乱数 R_{a2} を生成し、生成乱数 R_{a2} を情報処理装置500に送信する。

- 5 情報処理装置500は、ステップS575において、受信乱数 R_{a2} と生成乱数 R_{b2} とに基づいて、MAC値： $eK_m(R_{a2} \parallel R_{b2})$ を算出し、情報記録媒体ドライブ510に送信する。

- 10 情報記録媒体ドライブ510は、ステップS584において、受信した乱数 R_{b2} とステップS583において生成した乱数 R_{a2} とに基づいて、MAC値： $eK_m(R_{a2} \parallel R_{b2})$ を算出する。さらに、ステップS585において、算出したMAC値と、情報処理装置500から受信したMAC値とを比較する。一致すれば、情報記録媒体ドライブ510は、情報処理装置500が正しい認証キーを持つ正規なデバイスであると認証する。不一致の場合は、認証
15 エラーであり、その後の処理を中止する。

さらに、情報処理装置500は、ステップS576において、乱数 R_{a3} を生成して情報記録媒体ドライブ510に送信する。

- 20 情報記録媒体ドライブ510は、ステップS586において、乱数 R_{a3} を生成し、ステップS587において、生成乱数 R_{a3} と情報処理装置500からの受信乱数 R_{b3} との連結データに対する共有認証キー K_m を適用したAES暗号処理を実行し、セッションキー $K_s = eK_m(R_{a3} \parallel R_{b3})$ を算出する。

25

情報処理装置500は、ステップS577において、生成乱数 R_{b3} と情報記録媒体ドライブ510からの受信乱数 R_{a3} との連結データに対する共有認証キー K_m を適用したAES暗号処理を実行し、セッションキー $K_s = eK_m(R_{a3} \parallel R_{b3})$ を算出する。

上述した処理により、情報処理装置 500 と情報記録媒体ドライブ 510 とは、相互に正しいデバイスであることを確認し、セッションキー $K_s = e K_m (R a 3 \parallel R b 3)$ を共有することができる。図 17 に示すステップ S 560、
5 S 561 の処理が図 19 を参照して説明した処理に対応する。

上述した処理によって、セッションキー K_s が情報処理装置 500 と情報記録媒体ドライブ 510 とによって共有されると、図 17 に示すステップ S 562、S 563 の暗号化処理が情報記録媒体ドライブ 510 によって実行される。

10

ステップ S 562 の暗号化処理は、ステップ S 555 において生成した記録キー K_2 をセッションキー K_s で暗号化 (AES 暗号化) し、暗号化記録キー $e K_s (K_2)$ を生成する処理である。ステップ S 563 は、ステップ S 558 におけるブロックキー $K_b 1$ を適用した復号処理の結果取得された復号 TS
15 S パケット 604 をセッションキー K_s によって暗号化する処理である。なお、この場合、暗号化する対象は、TS パケット 604 全体である場合、一部である場合、シード情報 (シード 2) のみである場合など、処理態様は、TS パケットに含まれる秘密にすべき情報の格納態様、すなわちブロックキー $K_b 1$ によって暗号化された範囲に応じて決定してよい。これらの各態様は、図 13 ~
20 図 15 を参照して説明したとおりである。

ステップ S 562 において、記録キー K_2 のセッションキー K_s による暗号化データが生成され、ステップ S 563 において、シード情報 (シード 2) を含む秘密情報がセッションキー K_s によって暗号化され、これらの暗号化データ (図 18 の TS パケット 605) が情報記録媒体ドライブ 510 から、情報
25 処理装置 500 に送信される。すなわち、データ通信路において、転送されるデータはセッションキー K_s によって暗号化されたデータとなる。

情報処理装置 500 は、情報記録媒体ドライブ 510 から、これらのデータ

を受信すると、ステップS564およびステップS565において、受信暗号化データを復号する。すなわち、ステップS564において、セッションキー K_s を適用して暗号化記録キー eK_s (K_2)を復号して記録キー K_2 を取得し、ステップS565において、セッションキー K_s を適用してシード情報(シード2)を含む秘密情報を復号してシード情報(シード2)を含む秘密情報を取得する。図18に示すTSパケット606が復号されたシード情報(シード2)を含む。

ステップS566は、復号されたシード情報(シード2)と、ブロックキー K_b2 による復号対象データと、非暗号化データとを分離するセレクトステップである。ステップZS567(図17, 図18参照)では、ステップS565におけるセッションキー K_s を適用した復号処理の結果取得されたシード情報(シード2)と、ステップS564において生成した記録キー K_2 とに基づいて、AES暗号処理を実行し、ブロックキー K_b2 を算出する。

15

次に、ステップS568において、ブロックキー K_b2 を適用してユーザデータ部の暗号化部(ブロックキー K_b2 で暗号化されたデータ領域)を復号し、復号TSパケット群607を生成する。

20 復号TSパケット群607、および復号TSパケット606は、セレクトステップS569において結合されて、復号TSパケットとして例えばMP EG2デコーダに入力され、デコードされた後、再生される。

25 このように、本構成においては、情報記録媒体に格納されたデータの再生処理において、暗号化コンテンツの復号に適用する鍵(ブロックキー K_b2)を生成するために必要となるシード情報(シード2)をデバイス間で転送することが必要となる構成において、ブロックキー K_b2 の生成に必要なシード情報(シード2)および記録キー K_2 の双方をセッションキーで暗号化して送受信する構成としたので、転送路からのデータ漏洩が発生した場合であっても、

シード情報（シード2）および記録キーK2を取得することは困難であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。これは、情報処理装置500の中で、例えば記録キーK1の取得方法からブロックキーKb1の算出方法、そして、セッションキーKsの生成方法、および、セッションキーKsによる暗号化方法を一つのLSIパッケージ内の処理として秘匿性を高めることによって、一層強固なものとなる。

10 5 なお、前述した例と同様、2つのシード情報の格納形態には、様々な態様があり、以下、複数の例について説明する。

15 図20に、シード情報（シード1）と、シード情報（シード2）とを共にユーザデータ内の先頭TS packets 602内に格納した例を示す。先に図18を参照して説明した例では、シード情報（シード1）611が制御データ601に格納され、シード情報（シード2）612がユーザデータ内の先頭のTS packets 602内に暗号化されて格納された例を説明したが、図20に示す構成例は、シード情報（シード1）621、シード情報（シード2）622、双方がユーザデータ内の先頭のTS packets 602内に格納された例である。

20 20 なお、シード情報（シード2）622は、図18において説明した例と同様、シード情報（シード1）621を適用して取得されるブロックキーKb1によって暗号化されてユーザデータ内の先頭のTS packets 602内に格納される。

25 図20において、復号処理は、処理単位600を単位として実行される。この処理単位は、先に図1を参照して説明した（b）処理単位に相当する1ユニット（1AU: Aligned Unit）である。情報記録媒体520に格納された暗号化データの読み取りを実行する情報記録媒体ドライブ510は、制御データ内のフラグに基づいて、暗号処理単位である1AU (Aligned Unit)を抽出する。

図 20 の処理について説明する。図 20 において、図 17 の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

5 ステップ S 5 5 6 (図 17、図 20) は、情報記録媒体のユーザデータの先頭 TS パケット内から読み出したシード情報 (シード 1) 6 2 1 を AES 暗号処理部において、先のステップ S 5 5 4 (図 17 参照) において生成した記録キー K 1 を適用した AES 暗号処理を実行しブロックキー K b 1 生成処理を実行する。

10

次に、図 17 のステップ S 5 5 7 において、3 2 TS パケットからなるユーザデータからブロックキー K b 1 による暗号化データ部のみが抽出される。ブロックキー K b 1 による暗号化データ部、非暗号化部がステップ S 5 5 7 において分離されて、暗号化部のみがステップ S 5 5 8 において復号される。非暗号化部は、ステップ S 5 5 8 をスキップし、ステップ S 5 5 9 において、再度セレクトステップにより復号データと連結され、ステップ S 5 6 3 においてセッションキーによって暗号化がなされる。

15

ステップ S 5 5 8 (図 17、図 20 参照) では、ステップ S 5 5 6 において生成したブロックキー K b 1 を適用した AES 復号処理を実行する。ステップ S 5 5 8 では、ブロックキー K b 1 を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭 TS パケット 6 0 2 の少なくともシード情報 (シード 2) を含むデータ領域がブロックキー K b 1 を適用した暗号処理のなされたデータ部である。従って、このシード情報 (シード 2) を含むデータ領域を対象としてブロックキー K b 1 を適用した復号処理を実行する。

20

25

この先頭 TS パケット 6 0 2 の暗号化データ領域には、他のユーザデータ部、すなわち、後続の 5 9 5 2 バイトの TS パケット群 6 0 3 の復号処理に適用す

るブロックキーK b 2を算出するために必要となるシード情報(シード2) 6 2 2が含まれている。すなわち、シード情報(シード2) 6 2 2は、ブロックキーK b 1を適用した暗号処理がなされた暗号化データとして先頭TSパケット6 0 2に記録されている。

5

ステップS 5 5 6における、ブロックキーK b 1を適用した復号処理の結果として、復号TSパケット6 0 4が算出され、その中にはシード情報(シード2)が含まれる。

10

図17のセレクトステップS 5 5 9は、ブロックキーK b 1を適用した復号処理の結果から、シード情報(シード2)を含む復号データと、その他のデータを結合して、暗号化ステップS 5 6 3に出力することを示している。

15

ステップS 5 6 3における暗号化処理は、情報記録媒体ドライブ5 1 0と、情報処理装置5 0 0との間で実行する相互認証処理の結果として双方で共有するセッションキーに基づいて実行する暗号処理である。相互認証処理は、情報記録媒体ドライブ5 1 0と、情報処理装置5 0 0とが共有する認証キーK m 5 3 0, 5 4 0に基づいて実行される。相互認証処理およびセッションキー共有処理は、図19を参照して説明した通りである。

20

認証が成立し、セッションキーK sが共有されると、図17、図20に示すステップS 5 6 2、S 5 6 3の暗号化処理が情報記録媒体ドライブ5 1 0によって実行される。すなわち、ステップS 5 6 2において、記録キーK 2のセッションキーK sによる暗号化データが生成され、ステップS 5 6 3において、シード情報(シード2)を含む秘密情報がセッションキーK sによって暗号化され、これらの暗号化データ(図20のTSパケット6 0 5)が情報記録媒体ドライブ5 1 0から、情報処理装置5 0 0に送信される。すなわち、データ通信路において、転送されるデータはセッションキーK sによって暗号化されたデータとなる。

25

情報処理装置 500 は、情報記録媒体ドライブ 510 から、これらのデータを受信すると、ステップ S 564 およびステップ S 565 において、受信暗号化データを復号する。すなわち、ステップ S 564 において、セッションキー K_s を適用して暗号化記録キー e K_s (K₂) を復号して記録キー K₂ を取得し、ステップ S 565 において、セッションキー K_s を適用してシード情報 (シード 2) を含む秘密情報を復号してシード情報 (シード 2) を含む秘密情報を取得する。図 20 に示す TS パケット 606 が復号されたシード情報 (シード 2) を含む。

10 ステップ S 566 は、復号されたシード情報 (シード 2) と、ブロックキー K_b 2 による復号対象データと、非暗号化データとを分離するセレクトステップである。ステップ Z S 567 (図 17, 図 20 参照) では、ステップ S 565 におけるセッションキー K_s を適用した復号処理の結果取得されたシード
15 情報 (シード 2) と、ステップ S 564 において生成した記録キー K₂ とに基づいて、AES 暗号処理を実行し、ブロックキー K_b 2 を算出する。

次に、ステップ S 568 において、ブロックキー K_b 2 を適用してユーザデータ部の暗号化部 (ブロックキー K_b 2 で暗号化されたデータ領域) を復号し、
20 復号 TS パケット群 607 を生成する。

復号 TS パケット群 607、および復号 TS パケット 606 は、セレクトステップ S 569 において結合されて、復号 TS パケットとして例えば MPEG 2 デコーダに入力され、デコードされた後、再生される。

25 このように、本構成においては、シード情報 (シード 1) と、シード情報 (シード 2) とを共にユーザデータ内の先頭 TS パケット内に格納し、ブロックキー K_b 2 を生成するために必要となるシード情報 (シード 2) は、シード情報 (シード 1) と、記録キー K₁ とに基づいて生成するブロックキー K_b 1 によ

って暗号化して格納する構成とした。

本構成においても、シード情報(シード2)のディスクからの直接読み取り、データ転送路からの読み取りを行うことは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。これは、情報処理装置500の中で、例えば記録キーK1の取得方法からブロックキーKb1の算出方法、そして、セッションキーKsの生成方法、および、セッションキーKsによる暗号化方法を一つのLSIパッケージ内の処理として秘匿性を高めることによって、一層強固なものとなる。

図21に示す例は、シード情報(シード1)631をユーザデータ内の先頭TS packets 602に格納し、シード情報(シード2)632をユーザデータ内の次のTS packets 641に格納した例である。

なお、シード情報(シード2)632は、図18、図20において説明した例と同様、シード情報(シード1)631を適用して取得されるブロックキーKb1によって暗号化されてユーザデータ内の第2のTS packets 641内に格納される。

図21において、復号処理は、処理単位600を単位として実行される。この処理単位は、先に図1を参照して説明した(b)処理単位に相当する1ユニット(1AU: Aligned Unit)である。

図21の処理について説明する。図21において、図17の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

ステップS556(図17、図21)は、情報記録媒体のユーザデータの先頭TS packets内から読み出したシード情報(シード1)631をAES暗号

処理部に入力し、先のステップS 5 5 4（図1 7参照）において生成した記録キーK 1を適用したA E S暗号処理を実行してブロックキーK b 1を生成する。

- 5 次に、図1 7のステップS 5 5 7において、3 2 T S パケットからなるユーザデータからブロックキーK b 1による暗号化データ部のみが抽出される。ブロックキーK b 1による暗号化データ部、非暗号化部がステップS 5 5 7において分離されて、暗号化部のみがステップS 5 5 8において復号される。非暗号化部は、ステップS 5 5 8をスキップし、ステップS 5 5 9において、再度
- 10 セレクタステップにより復号データと連結され、ステップS 5 6 3においてセッションキーによって暗号化がなされる。

- ステップS 5 5 8（図1 7、図2 1参照）では、ステップS 5 5 6において生成したブロックキーK b 1を適用したA E S復号処理を実行する。復号処理
- 15 対象は、ブロックキーK b 1を適用した暗号処理がなされているデータ領域であり、ユーザデータの先頭T S パケット中のシード情報（シード1）5 2 1を除くデータ領域の暗号化領域と、第2 T S パケット中の少なくともシード情報（シード2）6 3 2を含むデータ領域の復号処理が実行される。ブロックキーK b 1を適用した暗号処理のなされたデータ部をどのデータ領域とするか
- 20 ついては、いくつかのパターンがあり、これらについては前述した通りである。

- 本例では、第2のT S パケット6 4 1の暗号化データ領域に、他のユーザデータ部、すなわち、後続のT S パケット群6 4 2の復号処理に適用するブロックキーK b 2を算出するために必要となるシード情報（シード2）6 3 2が含まれる。すなわち、シード情報（シード2）6 3 2は、ブロックキーK b 1を適用した暗号処理がなされた暗号化データとして第2 T S パケット6 4 1に記録されている。
- 25

ステップS 6 0 6における、ブロックキーK b 1を適用した復号処理の結果

として、復号TSパケット604が算出される。その中にシード情報(シード2)が含まれる。

図17のセレクトステップS559は、ブロックキーKb1を適用した復号
5 処理の結果から、シード情報(シード2)を含む復号データと、その他のデータ
を結合して、暗号化ステップS563に出力することを示している。

ステップS563における暗号化処理は、情報記録媒体ドライブ510と、
情報処理装置500との間で実行する相互認証処理の結果として双方で共有
10 するセッションキーに基づいて実行する暗号処理である。相互認証処理は、情報
記録媒体ドライブ510と、情報処理装置500とが共有する認証キーKm
530、540に基づいて実行される。相互認証処理およびセッションキー共有
処理は、図19を参照して説明した通りである。

15 認証が成立し、セッションキーKsが共有されると、図17、図21に示す
ステップS562、S563の暗号化処理が情報記録媒体ドライブ510によ
って実行される。すなわち、ステップS562において、記録キーK2のセ
ッションキーKsによる暗号化データが生成され、ステップS563において、
シード情報(シード2)を含む秘密情報がセッションキーKsによって暗号化
20 され、これらの暗号化データ(図21のTSパケット605)が情報記録媒体
ドライブ510から、情報処理装置500に送信される。すなわち、データ通
信路において、転送されるデータはセッションキーKsによって暗号化された
データとなる。

25 情報処理装置500は、情報記録媒体ドライブ510から、これらのデータ
を受信すると、ステップS564およびステップS565において、受信暗号
化データを復号する。すなわち、ステップS564において、セッションキー
Ksを適用して暗号化記録キーeKs(K2)を復号して記録キーK2を取得
し、ステップS565において、セッションキーKsを適用してシード情報(シ

ード2)を含む秘密情報を復号してシード情報(シード2)を含む秘密情報を取得する。図21に示すTSパケット606が復号されたシード情報(シード2)を含む。

- 5 ステップS566は、復号されたシード情報(シード2)と、ブロックキーKb2による復号対象データと、非暗号化データとを分離するセレクトステップである。ステップZS567(図17, 図21参照)では、ステップS565におけるセッションキーKsを適用した復号処理の結果取得されたシード情報(シード2)と、ステップS564において生成した記録キーK2とに基づいて、AES暗号処理を実行し、ブロックキーKb2を算出する。
- 10

次に、ステップS568において、ブロックキーKb2を適用してユーザデータ部の暗号化部(ブロックキーKb2で暗号化されたデータ領域)を復号し、復号TSパケット群607を生成する。

15

復号TSパケット群607、および復号TSパケット606は、セレクトステップS569において結合されて、復号TSパケットとして例えばMPEG2デコーダに入力され、デコードされた後、再生される。

- 20 このように、本構成においては、シード情報(シード1)ユーザデータ内の先頭TSパケット内に格納し、ブロックキーKb2を生成するために必要となるシード情報(シード2)をユーザデータ内の第2TSパケット内に格納し、シード情報(シード2)を、シード情報(シード1)と、記録キーK1とに基づいて生成するブロックキーKb1によって暗号化して格納する構成とした。

25

本構成においても、シード情報(シード2)をディスクから直接読み取ること、データ転送路からの読み取りを行うことは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。これは、情報処

理装置 500 の中で、例えば記録キー K1 の取得方法からブロックキー K b 1 の算出方法、そして、セッションキー K s の生成方法、および、セッションキー K s による暗号化方法を一つの L S I パッケージ内の処理として秘匿性を高めることによって、一層強固なものとなる。

5

〔他のデータ構成における適用〕

上述した例では、情報記録媒体に格納するデータを T S パケットとした例を説明したが、本発明の構成は、T S パケット以外の様々なデータ構成においても適用可能である。すなわち、暗号化データをブロック単位で暗号化するための第 2 のシード情報（シード 2）を、他のシード情報（シード 1）を適用して生成するブロックキー K b 1 によって暗号化して情報記憶媒体に格納する構成により、第 2 のシード情報（シード 2）の漏洩が防止され、セキュリティの高いコンテンツ保護が実現される。これは、トランスポートストリーム以外のデータ構成とした場合もブロック単位の暗号化処理を適用し、シード情報を用いたブロックキーを生成する構成であれば有効となる。

10
15

また、インタフェースを介したデータ転送の際にセッションキーによるデータ暗号化を行う構成例において、上述した例では、2つのシード情報中、一方をセッションキーによって暗号化する処理例を説明したが、セッションキーによるデータ暗号化を伴うデータ転送処理は、上述した構成例に限らず、一般的な暗号化コンテンツ格納構成においても有効である。

20

暗号化されていないシード情報を記録媒体上に持つ構成において、情報処理装置と、情報記録媒体ドライブ間で、データ転送を実行する処理例について、図 22 を参照して説明する。

25

図 22 に示す処理例において、情報記録媒体 670 には、暗号化コンテンツ 675 が記録され、暗号化コンテンツ 675 は、処理単位毎に設定されるシード情報 674 によって生成されるブロックキー K b 1 で暗号化されて記録さ

れている。

情報記録媒体ドライブ 660 において、暗号化コンテンツを格納した情報記録媒体 670 のデータを読み出し、PC 等の情報処理装置 650 において再生
5 する場合の処理を説明する。

情報記録媒体ドライブ 660 は自身のメモリに格納しているマスターキー 661 を読み出す。なお、マスターキー 661 は、情報処理装置 650 側に格納されている場合は、情報処理装置 650 から情報記録媒体ドライブ 660 に
10 送信してもよい。マスターキー 661 は、ライセンスを受けた情報処理装置(情報記録媒体ドライブを含む)に格納された秘密キーであり、複数の情報処理装置に共通なキーとして格納された共通キーである。

情報記録媒体ドライブ 660 は、ディスク ID (Disc ID) 671 を情報記録媒体 670 から読出す。ディスク ID (Disc ID) 671 は、ディスク固有
15 情報であり、例えば一般データ格納領域または、リードインエリアに格納される。

次に、情報記録媒体ドライブ 660 は、ステップ S 651 において、マスター
20 ーキー 661 とディスク ID 671 を用いて、ディスク固有キー (Disc Unique Key) を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法は、先に図 4 を参照して説明したと同様の方法が適用できる。

次に、記録コンテンツごとの固有鍵であるタイトルキー (Title Key) 1,
25 672 を情報記録媒体 670 から読出す。ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーが格納されている。

次にステップ S 652 において、ディスク固有キー (Disc Unique Key) と

タイトルキー (Title Key) 1, 672 から、タイトル固有キー (Title Unique Key) 1 を生成する。

5 さらに、情報記録媒体ドライブ 660 は、ステップ S652 において生成したタイトル固有キー (Title Unique Key) 1 と、情報記録媒体 670 から読み出した物理インデックス 673 とに基づいて、ステップ S653 において、記録キー (REC キー) K1 を生成する。

10 ステップ S653 において実行する記録キー (REC キー) K1 の生成処理は、先に図 5 を参照して説明した通り、タイトル固有キー (Title Unique Key) 1 と、情報記録媒体 670 から読み出した物理インデックス 673 とに基づく AES (Advanced Encryption Standard) 暗号処理により生成される。

15 ステップ S654 のブロックキー Kb1 の生成処理においては、情報記録媒体 670 からブロックキー Kb1 生成情報としてのシード情報 674 を読み出し、シード情報 674 と、ステップ S653 において生成した記録キー K1 とに基づく暗号処理を実行してブロックキー Kb1 を生成する。

20 ステップ S654 のブロックキー Kb1 の生成処理以降に実行する処理について、図 23 を参照して説明する。

図 23 において、復号処理は、例えば 2048 バイトの処理単位内のユーザデータ 701 を単位として実行される。処理単位毎に制御データ 711 が設定される。情報記録媒体ドライブ 660 は、制御データ内のフラグに基づいて、25 暗号処理単位である 1 AU (Aligned Unit) を抽出する。

処理単位には、18 バイトの制御データ 711 と、2048 バイトの暗号化ユーザデータ 701 が含まれる。シード情報 674 が制御データ 711 内に格納されている。暗号化ユーザデータ 701 は、シード情報 721 に基づいて生

成されるブロックキーK b 1によって暗号化されたデータである。

図23において、図22の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

5

ステップS654(図22、図23)は、情報記録媒体の制御データ内から読み出したシード情報674をAES暗号処理部に入力し、先のステップS653において生成した記録キーK1を適用したAES暗号処理を実行しブロックキーK b 1生成処理を実行するステップである。

10

ステップS655(図22、図23参照)では、ステップS654において生成したブロックキーK b 1を適用したAES復号処理を実行する。ステップS655では、ブロックキーK b 1を適用した暗号処理のなされたユーザデータ701を対象とした復号処理が実行される。例えばAESのCBC(Cipher Block Chaining)モードを適用した処理を実行する。

15

次のステップS663における暗号化処理は、情報記録媒体ドライブ660と、情報処理装置650との間で実行する相互認証処理の結果として双方で共有するセッションキーに基づいて実行する暗号処理である。相互認証処理は、情報記録媒体ドライブ660と、情報処理装置650とが共有する認証キーK m 680, 690に基づいて実行される。相互認証処理のシーケンスは、例えば先に図19を参照して説明したシーケンスに従って実行される。

20

図22に示すステップS661、S662において、相互認証処理、セッションキーK s生成が実行され、情報処理装置650と情報記録媒体ドライブ660とによってセッションキーK sが共有される。

25

次に、ステップS663(図22、図23参照)の暗号化処理が情報記録媒体ドライブ660によって実行される。

ステップS 6 6 3の暗号化処理は、ステップS 6 5 5において復号処理の結果取得された復号ユーザデータをセッションキーK sによって暗号化する処理である。例えばAESのCBC (Cipher Block Chaining) モードを適用した暗号化処理を実行し、暗号化ユーザデータ7 0 2を生成する。

この暗号化データ(図2 3のユーザデータ7 0 2)が情報記録媒体ドライブ6 6 0から、情報処理装置6 5 0に送信される。すなわち、データ通信路において、転送されるデータはセッションキーK sによって暗号化されたデータとなる。

情報処理装置6 5 0は、情報記録媒体ドライブ6 6 0から、暗号化ユーザデータを受信すると、ステップS 6 6 4において、受信暗号化データを復号する。すなわち、セッションキーK sを適用して例えばAESのCBC (Cipher Block Chaining) モードを適用した復号処理を実行し、ユーザデータ7 0 3を取得する。

この例においても、情報記録媒体に格納されたデータの再生処理において、デバイス間の転送データをセッションキーで暗号化して送受信する構成としたので、転送路において盗聴等が発生した場合であっても、コンテンツの漏洩は防止され、セキュリティレベルの高いコンテンツ保護が実現される。これは、情報処理装置5 0 0の中で、例えば記録キーK 1の取得方法からブロックキーK b 1の算出方法、そして、セッションキーK sの生成方法、および、セッションキーK sによる暗号化方法を一つのLSIパッケージ内の処理として秘匿性を高めることによって、一層強固なものとなる。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきた

のであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

5 なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

10 例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory) に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) ディスク, DVD (Digital Versatile Disc)、磁気ディスク、半導体
15 メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

20 なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

25 なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限

らない。

産業上の利用可能性

- 5 以上、説明したように、本発明の構成によれば、暗号化コンテンツの復号に適用する鍵(ブロックキー K_b2)を生成するために必要となるシード情報(シード2)を他の鍵(ブロックキー K_b1)によって暗号化して格納する構成としたので、シード情報(シード2)をディスクから直接読み取ることは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現
- 10 される。

- さらに、本発明の構成によれば、情報記録媒体に格納されたデータの再生処理において、暗号化コンテンツの復号に適用する鍵(ブロックキー K_b2)生成用のシード情報(シード2)をデバイス間で転送することが必要となる構成
- 15 において、ブロックキー生成情報、具体的には、シード情報(シード2)および記録キー K_2 の双方をセッションキーで暗号化して送受信する構成としたので、転送路からのデータ漏洩が発生した場合であっても、シード情報(シード2)および記録キー K_2 を取得することは困難となり、シード情報を用いて
- 20 生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

請求の範囲

1. 情報記録媒体に格納された暗号化データの復号処理を実行する情報処理装置であり、
情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキー K_b1 を生成し、生成した第1ブロックキー K_b1 に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードに基づいて第2ブロックキー K_b2 を生成し、生成した第2ブロックキー K_b2 に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する暗号処理手段を有する情報処理装置。
2. 前記情報処理装置は、
マスターキー生成情報を格納した記憶手段を有し、
前記暗号処理手段は、
前記マスターキー生成情報に基づいてマスターキーを生成し、該生成したマスターキーと前記情報記録媒体からの読み出し情報とに基づいて、2つの記録キー $K1$ 、 $K2$ を生成し、生成した第1記録キー $K1$ と前記第1シード情報とに基づく暗号処理により前記第1ブロックキー K_b1 を生成し、生成した第1ブロックキー K_b1 に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードと第2記録キー $K2$ とに基づく暗号処理により前記第2ブロックキー K_b2 を生成し、生成した第2ブロックキー K_b2 に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する構成である請求項1に記載の情報処理装置。
3. 前記暗号処理手段は、
前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスク

I D、および前記情報記録媒体に記録された2つのタイトルキーに基づいて第1タイトル固有キーおよび第2タイトル固有キーを生成し、さらに、

前記第1タイトル固有キーと、前記情報記録媒体からの第1読み出し情報とに基づく暗号処理により前記第1記録キーK1を生成し、

- 5 前記第2タイトル固有キーと、前記情報記録媒体からの第2読み出し情報とに基づく暗号処理により前記第2記録キーK2を生成する構成である請求項2に記載の情報処理装置。

4. 前記暗号処理手段は、

- 10 前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクI D、および前記情報記録媒体に記録された1つのキーシード情報に基づいて第1タイトル固有キーおよび第2タイトル固有キーを生成し、さらに、

前記第1タイトル固有キーと、前記情報記録媒体からの第1読み出し情報とに基づく暗号処理により前記第1記録キーK1を生成し、

- 15 前記第2タイトル固有キーと、前記情報記録媒体からの第2読み出し情報とに基づく暗号処理により前記第2記録キーK2を生成する構成である請求項2に記載の情報処理装置。

5. 情報記録媒体に格納された暗号化データの読み取りおよび外部出力を
20 実行する情報記録媒体ドライブ装置であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキーKsを生成する認証処理部と、

- 情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキーKb1
25 を生成し、生成した第1ブロックキーKb1に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、前記セッションキーKsに基づいて前記第2シードを含むデータの暗号化処理を実行し出力用暗号化情報を生成する暗号処理手段とを有し、

前記セッションキーKsに基づいて暗号化された第2シードを含む出力用

暗号化情報をインタフェースを介して出力する構成を有する情報記録媒体ドライブ装置。

6. 前記暗号処理手段は、

- 5 情報記録媒体ドライブ装置の保有するマスターキー生成情報に基づいて生成したマスターキーと、前記情報記録媒体からの読み出し情報とに基づいて、2つの記録キーK1、K2を生成し、生成した第1記録キーK1と前記第1シード情報とに基づく暗号処理により前記第1ブロックキーKb1を生成し、生成した第1ブロックキーKb1に基づいて情報記録媒体に格納された暗号化
- 10 第2シードの復号処理を実行して第2シードを取得し、取得した第2シードと第2記録キーK2とを含むデータを前記セッションキーKsに基づいて暗号化して出力用暗号化情報を生成し、

- 前記第2シードと第2記録キーK2とを含む前記出力用暗号化情報をインタフェースを介して出力する構成を有する請求項5に記載の情報記録媒体
- 15 ライブ装置。

7. データ入力インタフェースを介して入力する暗号データの復号処理を実行する情報処理装置であり、

- 前記暗号データの出力装置との認証処理を実行しセッションキーKsを生成する認証処理部と、
- 20

- 前記データ入力インタフェースを介して入力する暗号化情報を前記セッションキーに基づく復号処理により鍵生成情報としてのシード情報および記録キーを取得し、前記シード情報および記録キーに基づく暗号処理により暗号データの復号キーとしてのブロックキーを生成し、該ブロックキーに基づく暗号
- 25 データの復号処理を実行する暗号処理部と、
- を有する情報処理装置。

8. 情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報記録媒体ドライブ装置であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキー K_s を生成する認証処理部と、

- 5 情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としてのシードに基づいてブロックキーを生成し、生成したブロックキーに基づいて情報記録媒体に格納された暗号化データの復号処理を実行して復号データを取得し、前記セッションキー K_s に基づいて前記復号データの暗号化処理を実行し出力用暗号化情報を生成する暗号処理手段とを有し、

- 10 前記セッションキー K_s に基づいて暗号化された出力用暗号化情報をインタフェースを介して出力する構成を有する情報記録媒体ドライブ装置。

9. 暗号化データを格納した情報記録媒体であり、

暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードと、

- 15 前記第1シードに基づいて生成される第1ブロックキー K_{b1} に基づいて暗号化された鍵生成情報としての暗号化第2シードと、

前記第2シードに基づいて生成される第2ブロックキー K_{b1} に基づいて暗号化された暗号化コンテンツと、

を格納した構成を有する情報記録媒体。

20

10. 前記第1シードは、前記暗号化処理単位毎に設定された制御情報内に格納され、

前記第2シードは、前記制御情報外のユーザデータ領域に暗号化されて格納された構成である請求項9に記載の情報記録媒体。

25

11. 前記第1シードは、ユーザデータ領域に非暗号化データとして格納され、

前記第2シードは、ユーザデータ領域に暗号化データとして格納された構成である請求項9に記載の情報記録媒体。

1 2. 前記暗号化データは、トランスポートストリームパケットから構成され、

5 前記第1シードは、複数のトランスポートストリームパケットに対応する制御情報内に格納され、前記第2シードは、前記制御情報外のユーザデータ領域のトランスポートストリームパケット内に暗号化されて格納された構成である請求項9に記載の情報記録媒体。

10 1 3. 前記暗号化データは、トランスポートストリームパケットから構成され、

前記第1シードは、ユーザデータ領域のトランスポートストリームパケット内に非暗号化データとして格納され、

前記第2シードは、ユーザデータ領域のトランスポートストリームパケット内に暗号化されて格納された構成である請求項9に記載の情報記録媒体。

15

1 4. 情報記録媒体に格納された暗号化データの復号処理を実行する情報処理方法であり、

20 情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキー $Kb1$ を生成するステップと、

生成した第1ブロックキー $Kb1$ に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードに基づいて第2ブロックキー $Kb2$ を生成するステップと、

25 生成した第2ブロックキー $Kb2$ に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップと、
を有する情報処理方法。

1 5. 前記情報処理方法は、さらに、

記憶手段から読み出したマスターキー生成情報に基づいて生成したマスタ

ーキーと、前記情報記録媒体からの読み出し情報とに基づいて、2つの記録キーK 1, K 2を生成するステップを有し、

- 5 生成した第1記録キーK 1と前記第1シード情報とに基づく暗号処理により前記第1ブロックキーK b 1を生成し、生成した第1ブロックキーK b 1に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードと第2記録キーK 2とに基づく暗号処理により前記第2ブロックキーK b 2を生成し、生成した第2ブロックキーK b 2に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する請求項14に記載の情報処理方法。

10

16. 前記情報処理方法は、

前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクID、および前記情報記録媒体に記録された2つのタイトルキーに基づいて第1タイトル固有キーおよび第2タイトル固有キーを生成し、さらに、

- 15 前記第1タイトル固有キーと、前記情報記録媒体からの第1読み出し情報とに基づく暗号処理により前記第1記録キーK 1を生成し、

前記第2タイトル固有キーと、前記情報記録媒体からの第2読み出し情報とに基づく暗号処理により前記第2記録キーK 2を生成するステップを有する請求項15に記載の情報処理方法。

20

17. 前記情報処理方法は、

前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクID、および前記情報記録媒体に記録された1つのキーシード情報に基づいて第1タイトル固有キーおよび第2タイトル固有キーを生成し、さらに、

- 25 前記第1タイトル固有キーと、前記情報記録媒体からの第1読み出し情報とに基づく暗号処理により前記第1記録キーK 1を生成し、

前記第2タイトル固有キーと、前記情報記録媒体からの第2読み出し情報とに基づく暗号処理により前記第2記録キーK 2を生成するステップを有する請求項15に記載の情報処理方法。

18. 情報記録媒体に格納された暗号化データの読み取りおよび外部出力
を実行する情報処理方法であり、

5 情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行
しセッションキー K_s を生成する認証処理ステップと、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設
定された鍵生成情報としての第1シードに基づいて第1ブロックキー K_{b1}
を生成するステップと、

10 生成した第1ブロックキー K_{b1} に基づいて情報記録媒体に格納された暗
号化第2シードの復号処理を実行して第2シードを取得し、前記セッションキ
ー K_s に基づいて前記第2シードを含むデータの暗号化処理を実行し出力用
暗号化情報を生成するステップと、

前記セッションキー K_s に基づいて暗号化された第2シードを含む出力用
暗号化情報をインタフェースを介して出力するステップと、

15 を有する情報処理方法。

19. 前記情報処理方法は、

情報記録媒体ドライブ装置の保有するマスターキー生成情報に基づいて生
成したマスターキーと、前記情報記録媒体からの読み出し情報とに基づいて、
20 2つの記録キー K_1 , K_2 を生成し、生成した第1記録キー K_1 と前記第1シ
ード情報とに基づく暗号処理により前記第1ブロックキー K_{b1} を生成し、生
成した第1ブロックキー K_{b1} に基づいて情報記録媒体に格納された暗号化
第2シードの復号処理を実行して第2シードを取得し、取得した第2シードと
第2記録キー K_2 とを含むデータを前記セッションキー K_s に基づいて暗号
25 化して出力用暗号化情報を生成し、

前記第2シードと第2記録キー K_2 とを含む前記出力用暗号化情報をイン
タフェースを介して出力する請求項18に記載の情報処理方法。

20. データ入力インタフェースを介して入力する暗号データの復号処理

を実行する情報処理方法であり、

前記暗号データの出力装置との認証処理を実行しセッションキー K_s を生成する認証処理ステップと、

- 5 前記データ入力インタフェースを介して入力する暗号化情報を前記セッションキーに基づく復号処理により鍵生成情報としてのシード情報および記録キーを取得し、前記シード情報および記録キーに基づく暗号処理により暗号データの復号キーとしてのブロックキーを生成し、該ブロックキーに基づく暗号データの復号処理を実行する暗号処理ステップと、
- を有する情報処理方法。

10

21. 情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報処理方法であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキー K_s を生成する認証処理ステップと、

15

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としてのシードに基づいてブロックキーを生成し、生成したブロックキーに基づいて情報記録媒体に格納された暗号化データの復号処理を実行して復号データを取得し、前記セッションキー K_s に基づいて前記復号データの暗号化処理を実行し出力用暗号化情報を生成する暗号処理ステップと、

20

前記セッションキー K_s に基づいて暗号化された出力用暗号化情報をインタフェースを介して出力するステップと、

を有する情報処理方法。

25

22. 情報記録媒体に格納された暗号化データの復号処理を実行するコンピュータ・プログラムであり、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第1シードに基づいて第1ブロックキー K_{b1} を生成するステップと、

生成した第1ブロックキーK b 1に基づいて情報記録媒体に格納された暗号化第2シードの復号処理を実行して第2シードを取得し、取得した第2シードに基づいて第2ブロックキーK b 2を生成するステップと、

- 生成した第2ブロックキーK b 2に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップと、
- 5 を有するコンピュータ・プログラム。

1/23

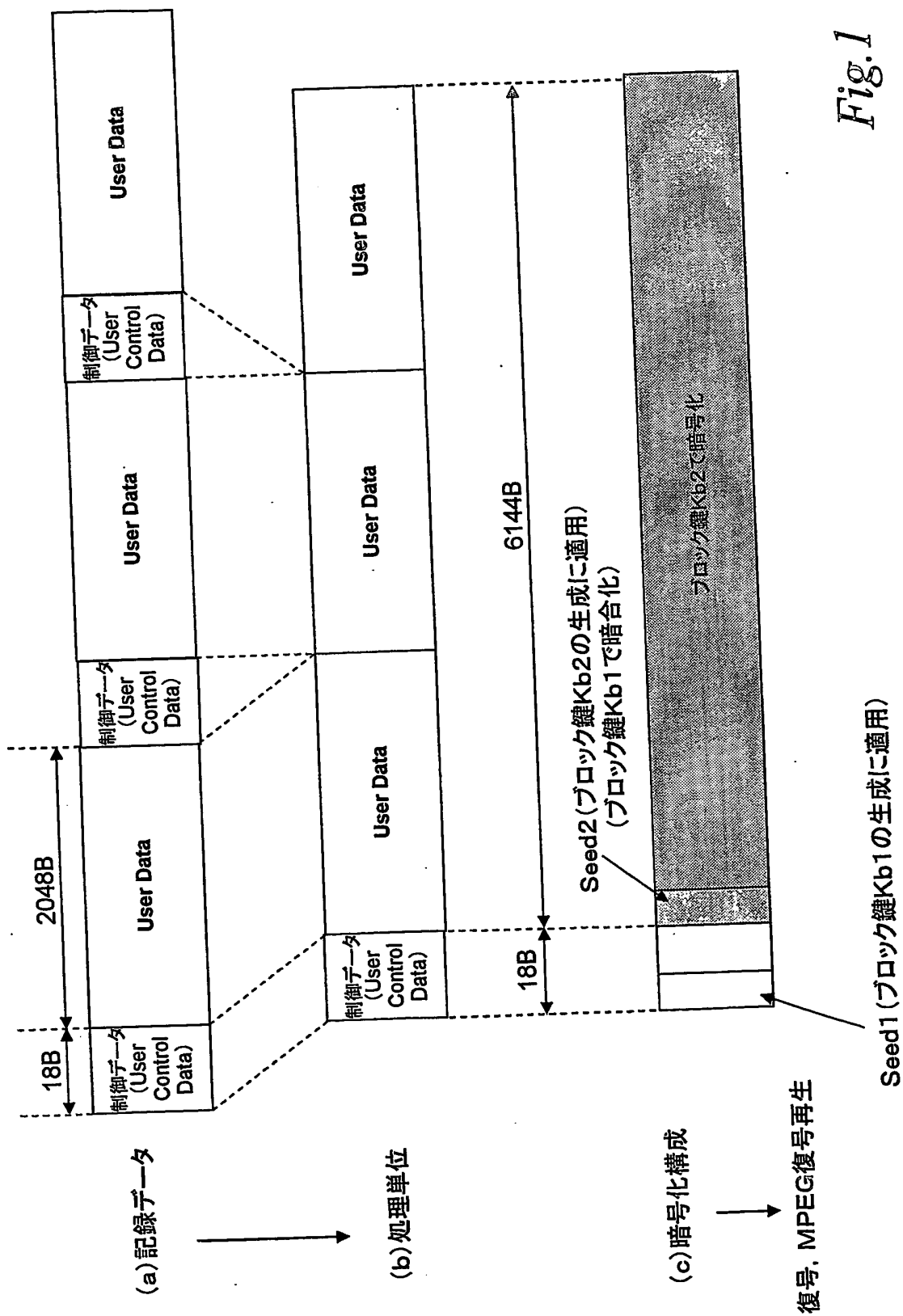


Fig. 1

2/23

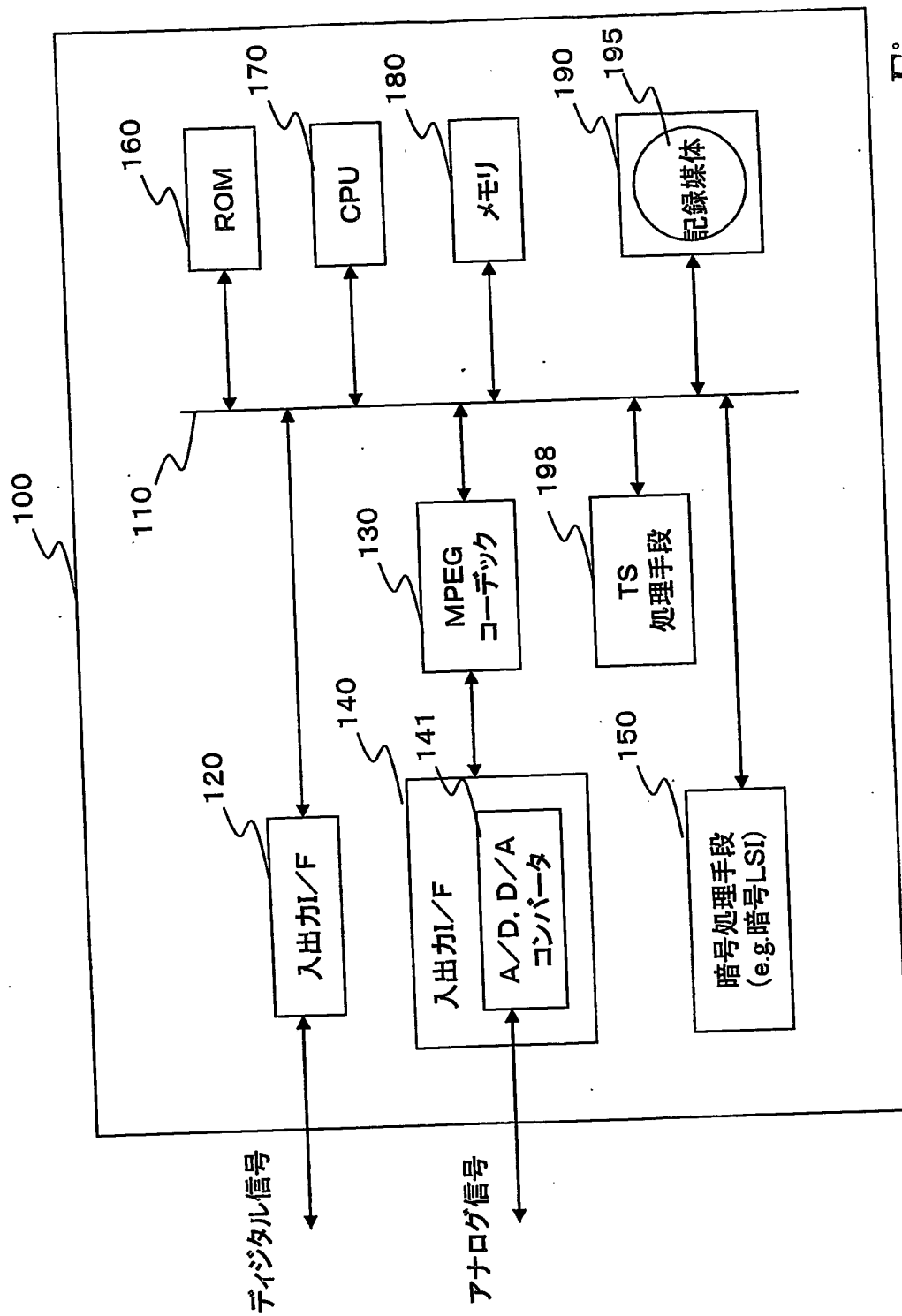
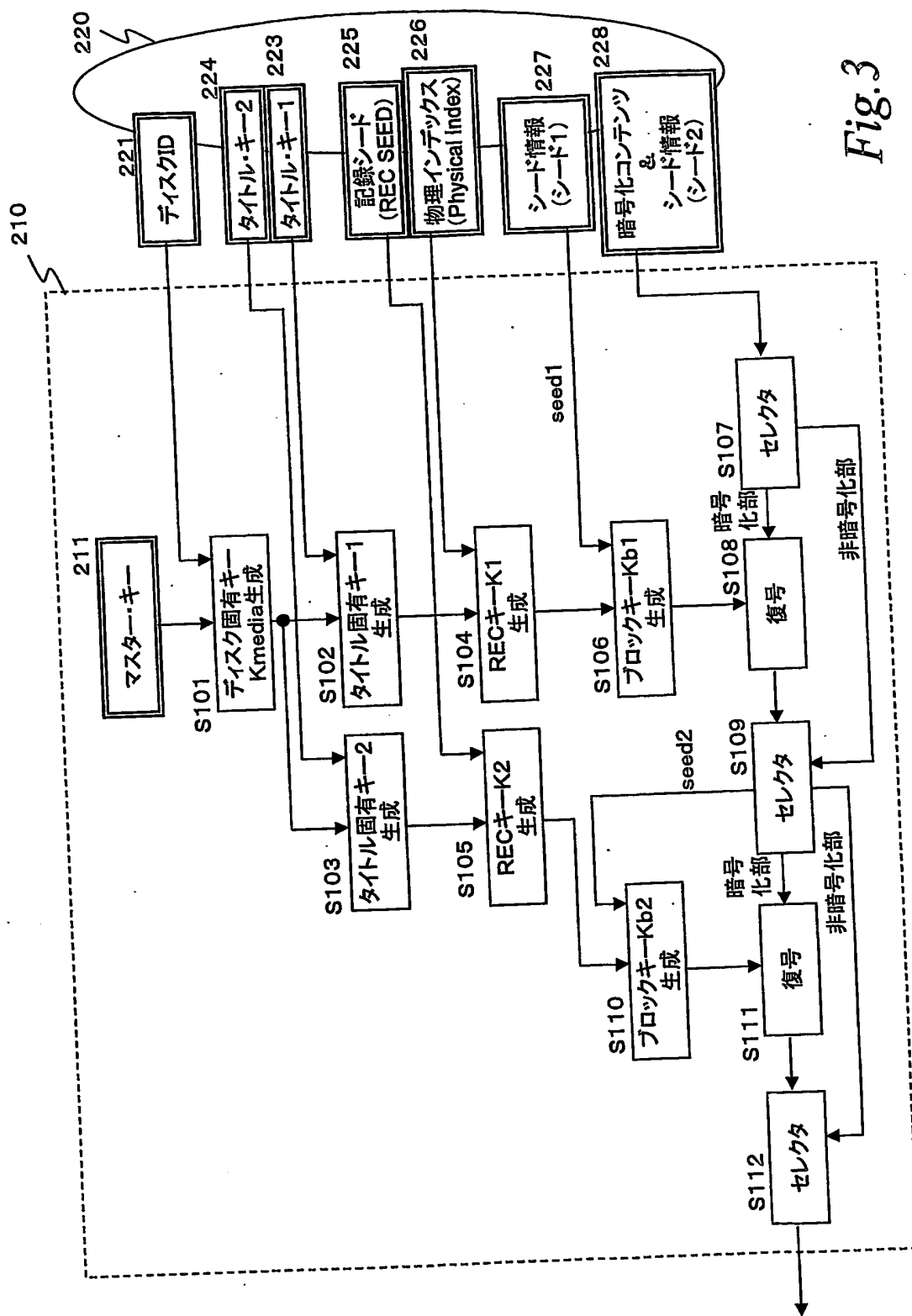


Fig. 2

3/23



4/23

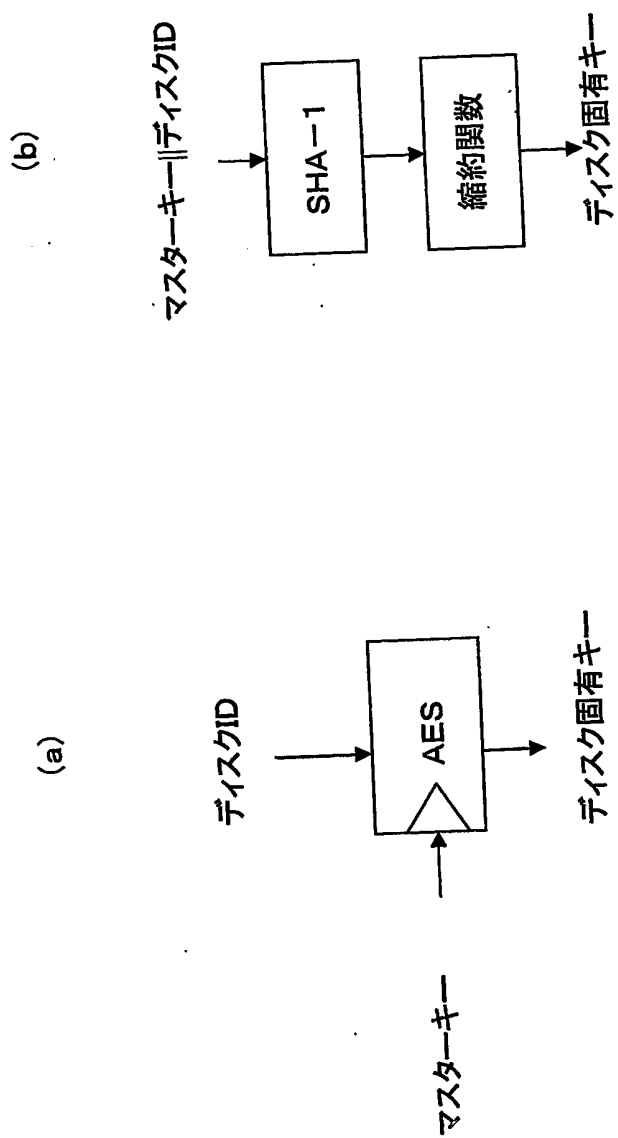


Fig. 4

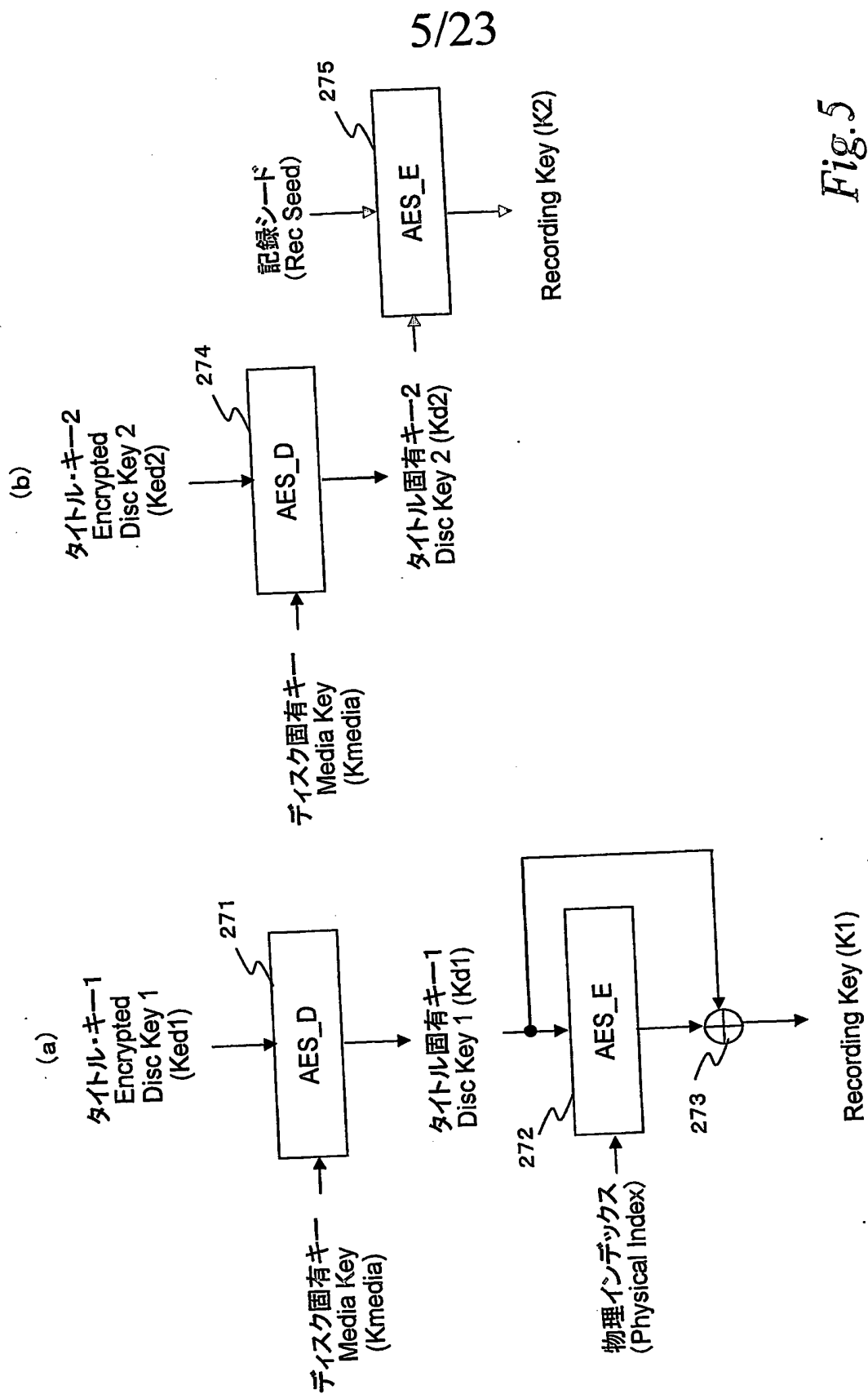


Fig. 5

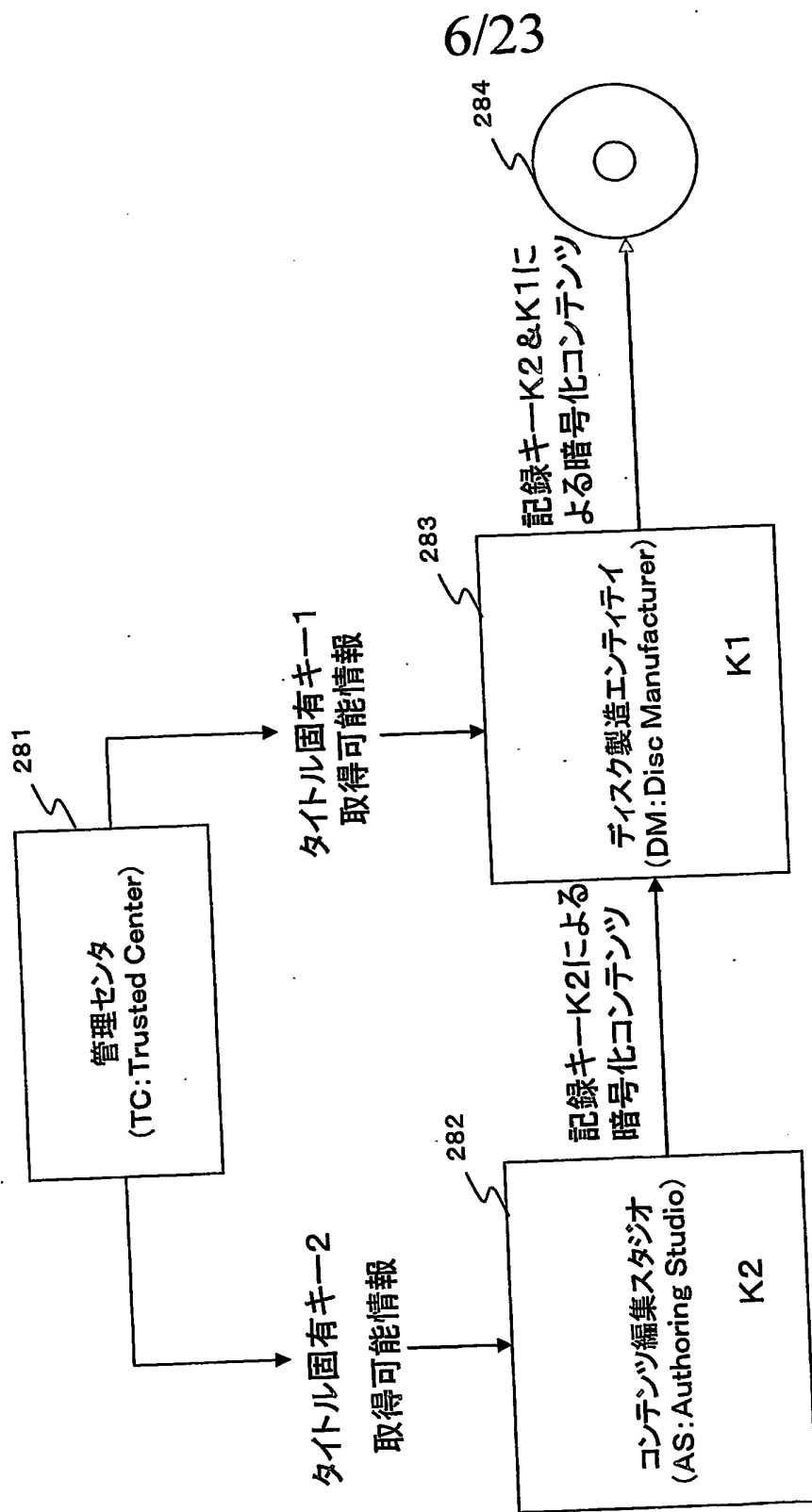


Fig. 6

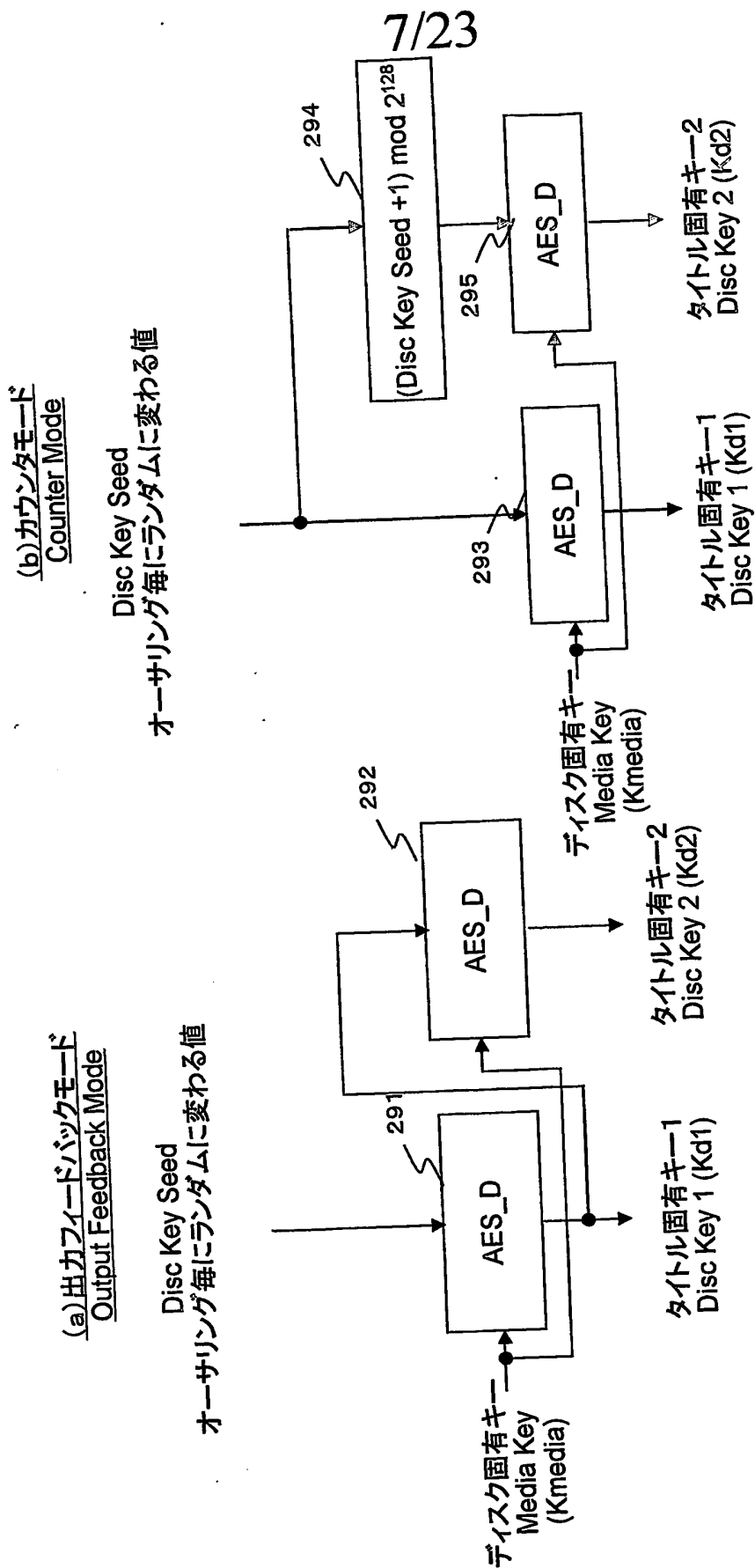
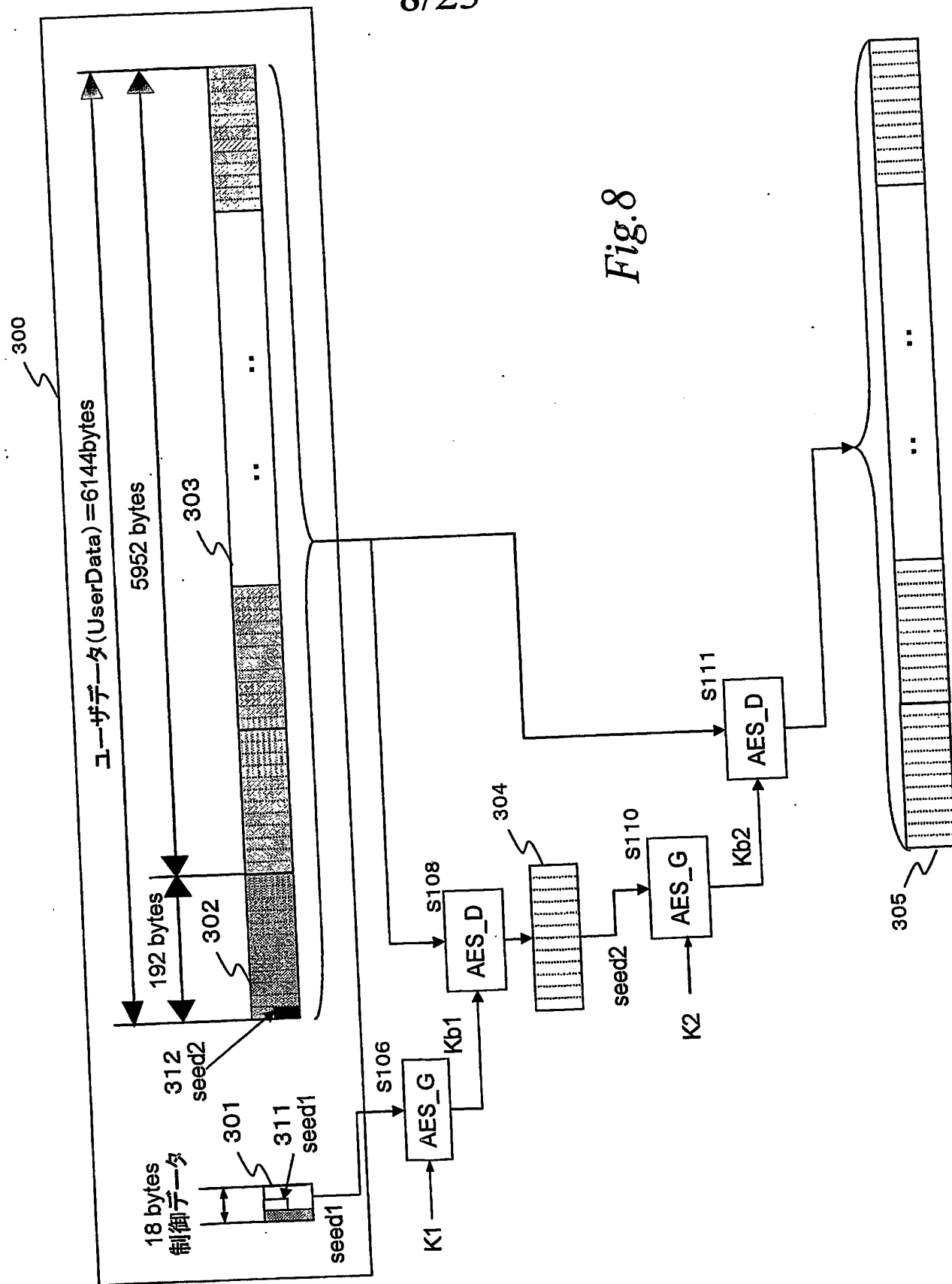
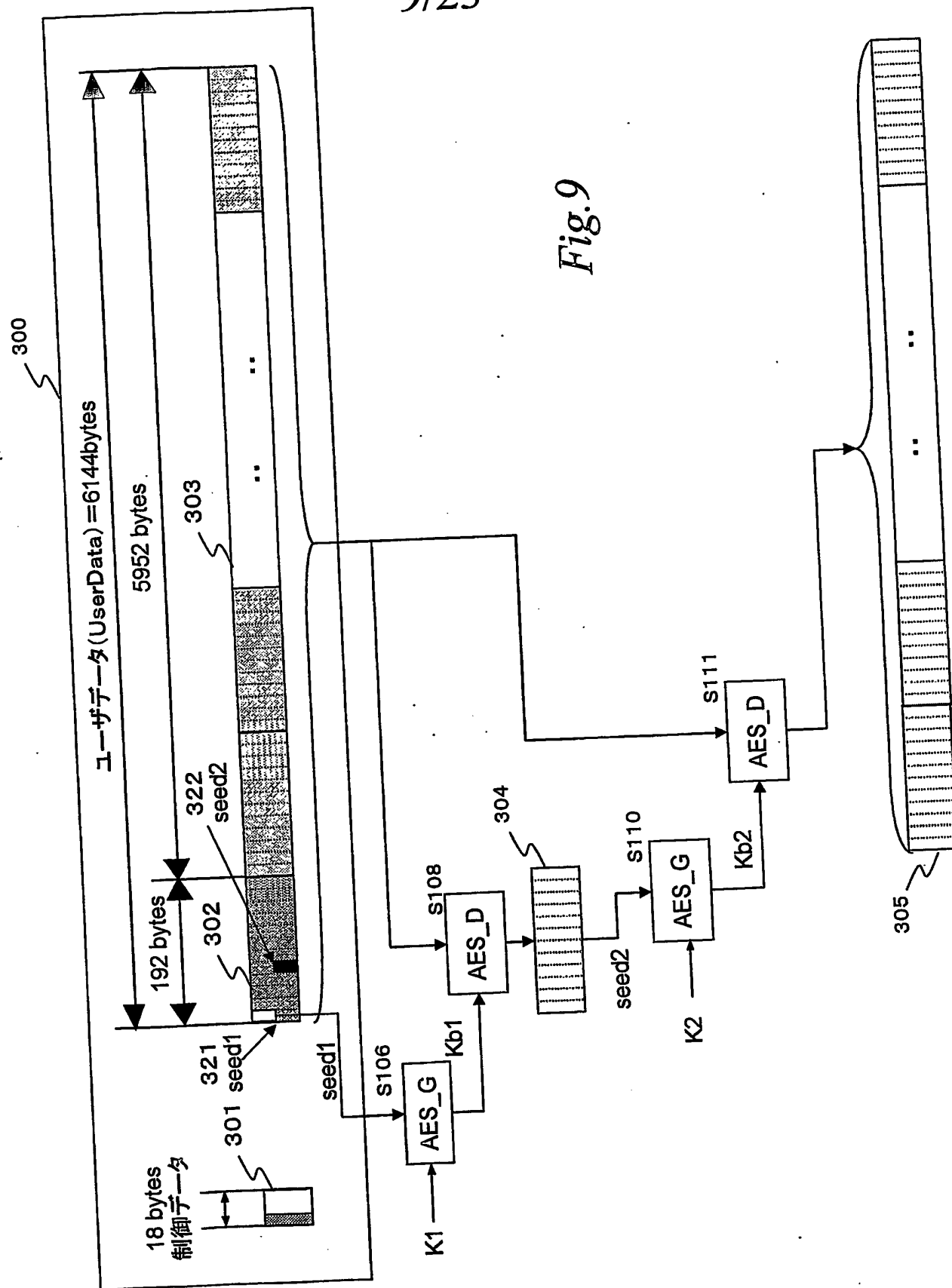


Fig. 7

8/23

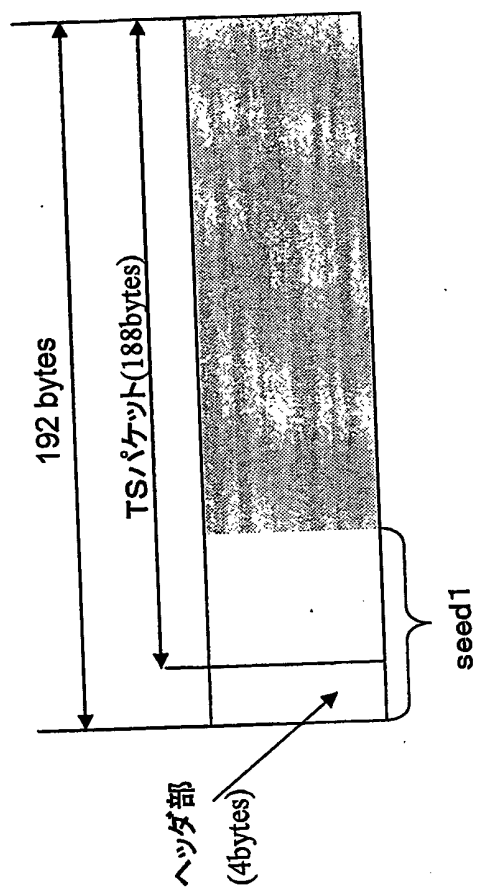


9/23



10/23

(a) 暗号化処理単位の先頭192byte(ヘッダ部+1TS/パケット)



(b) 暗号化処理単位の先頭4byte(ヘッダ部のみ)

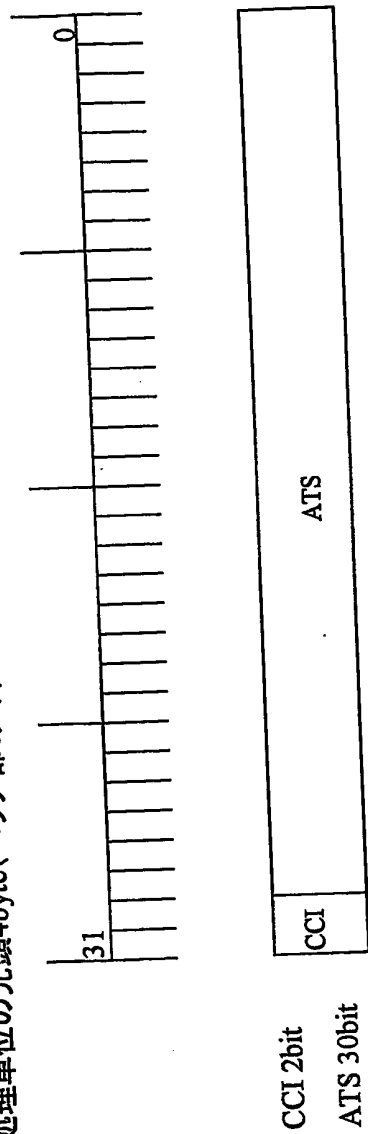
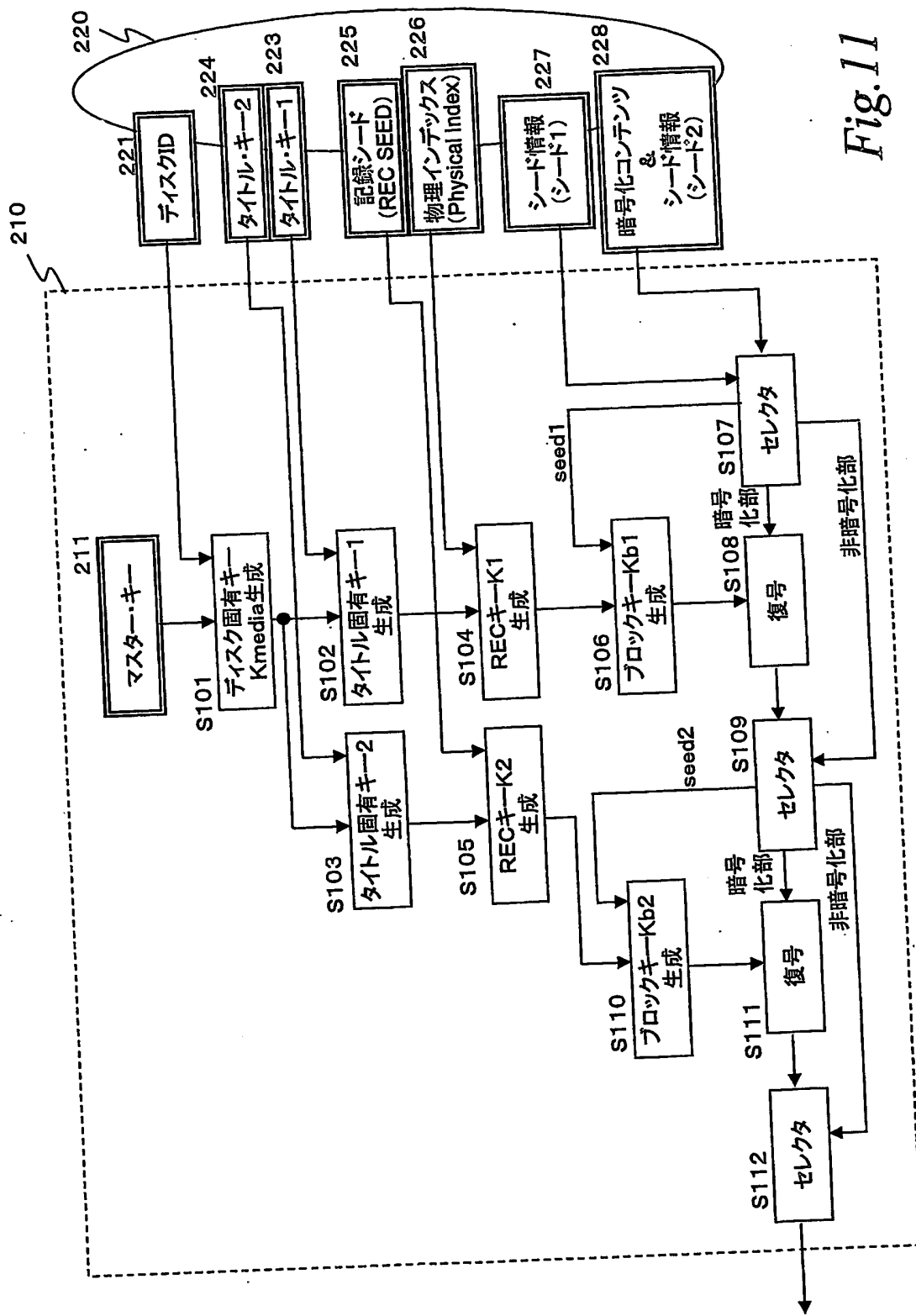


Fig.10

11/23



12/23

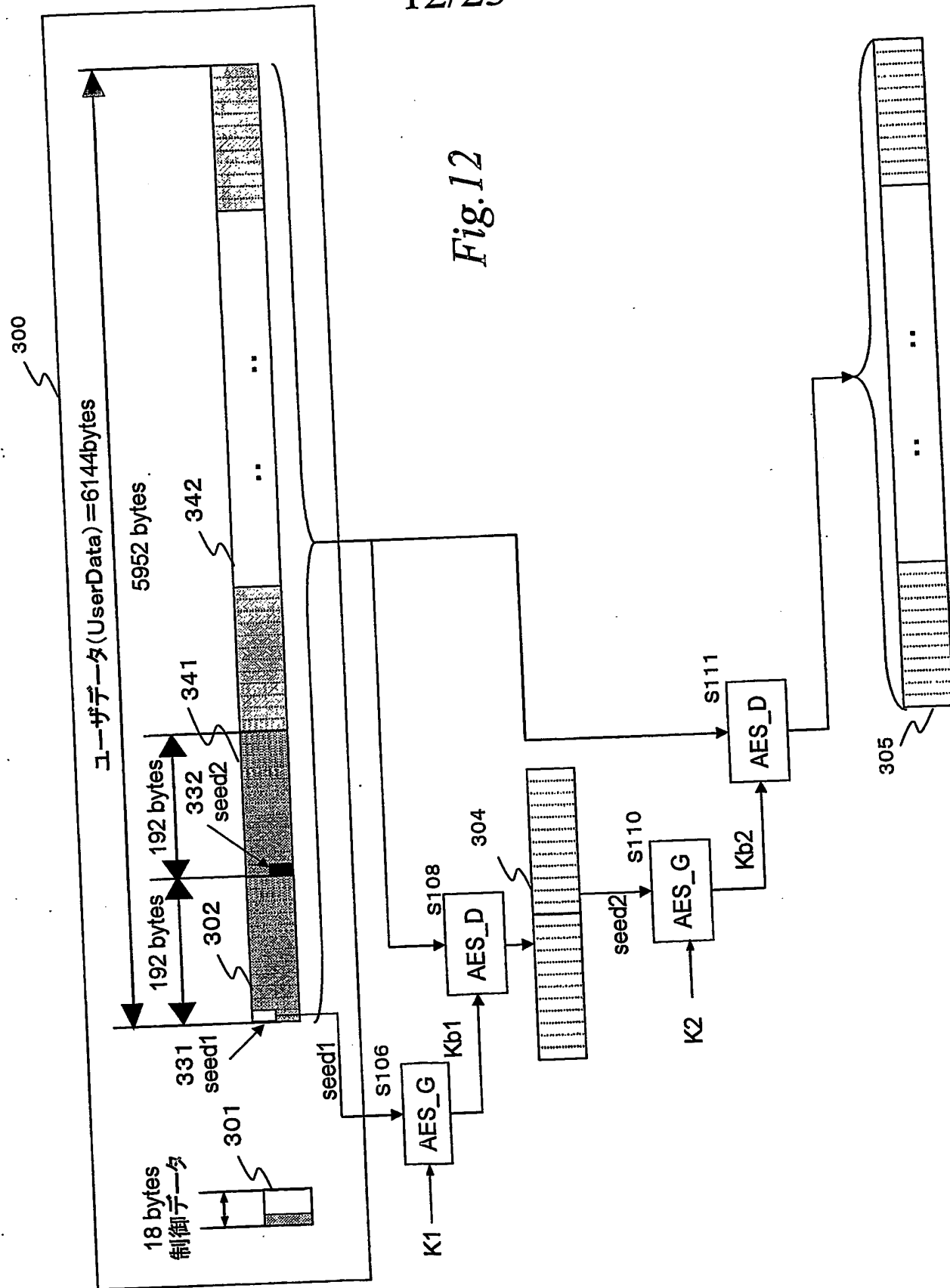


Fig. 13

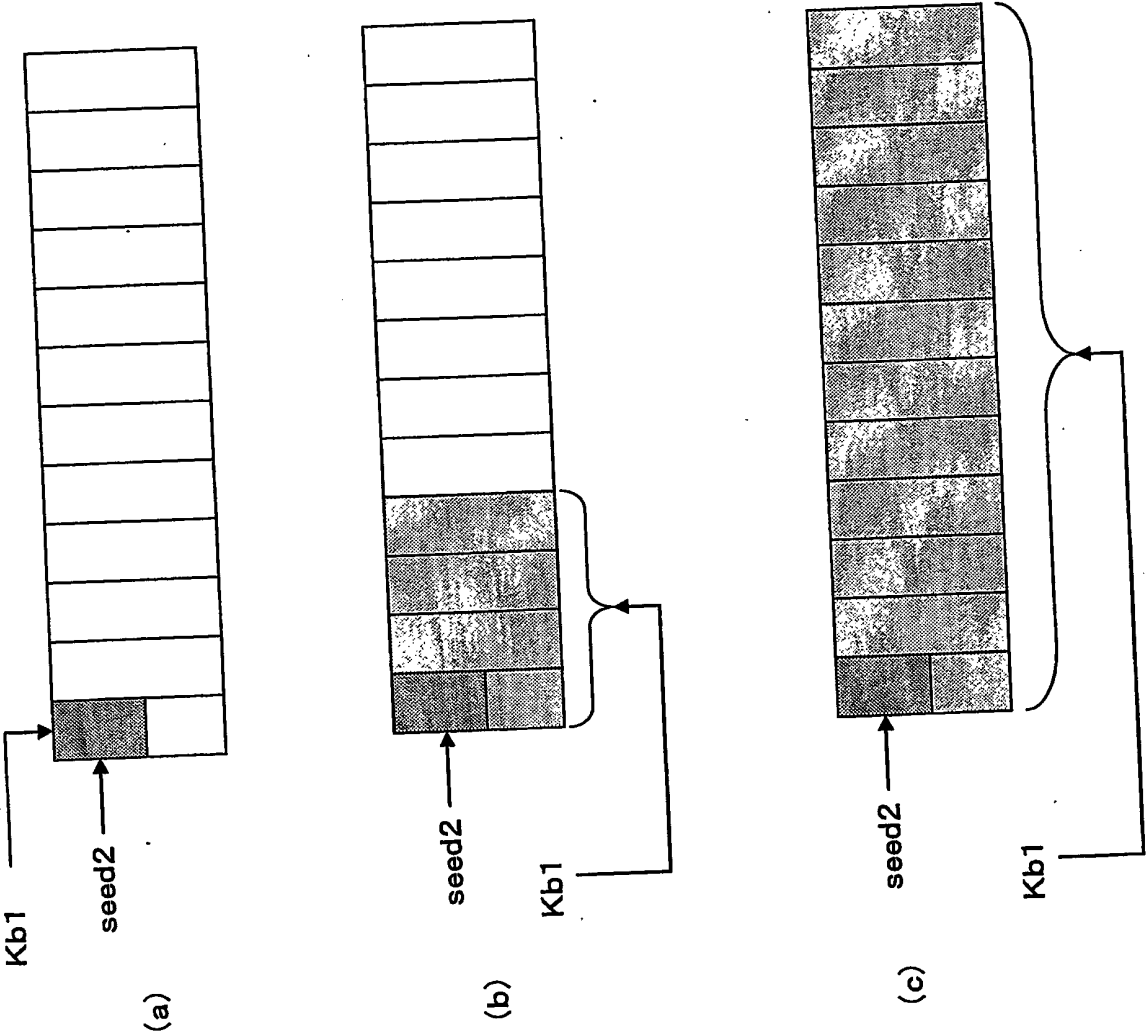
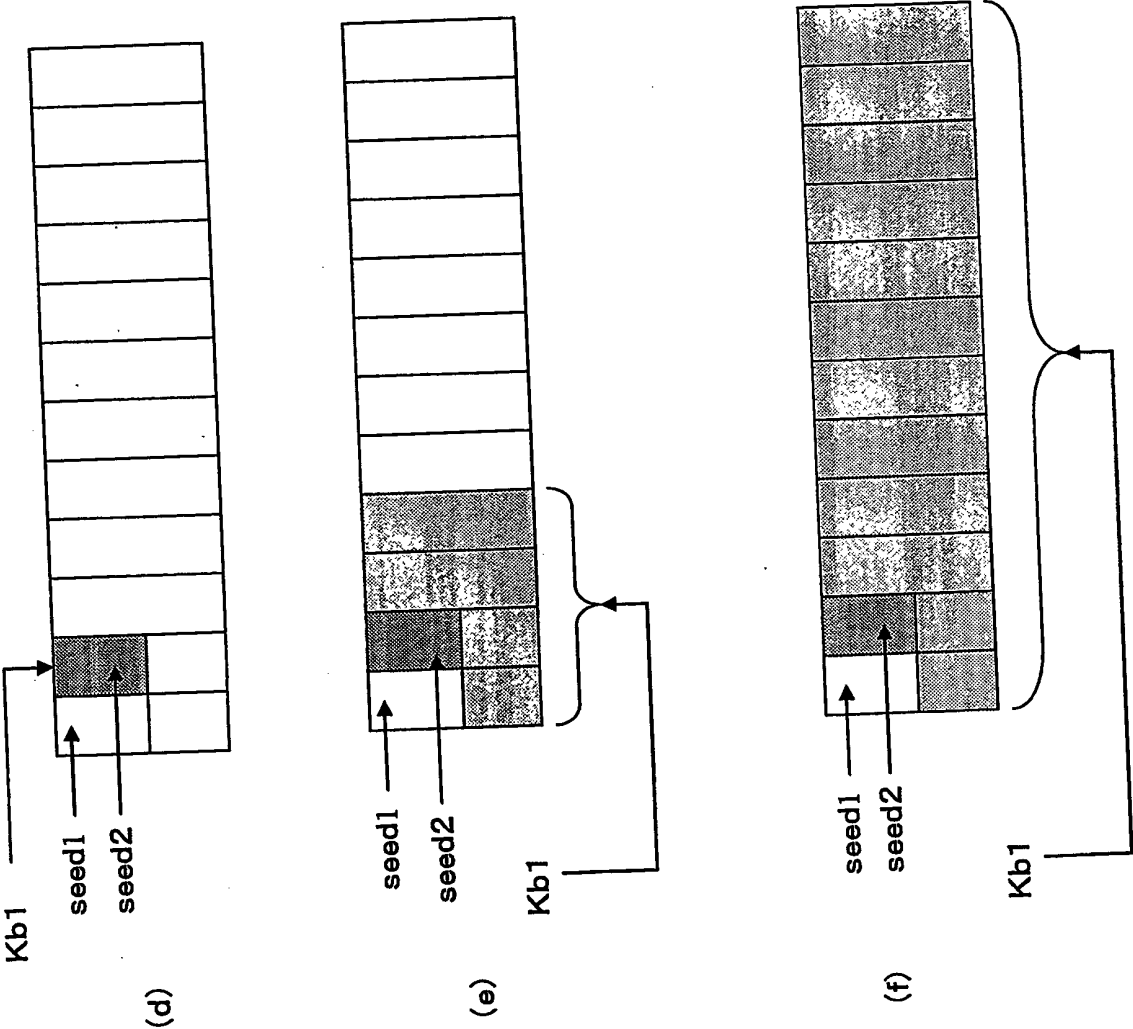


Fig. 14



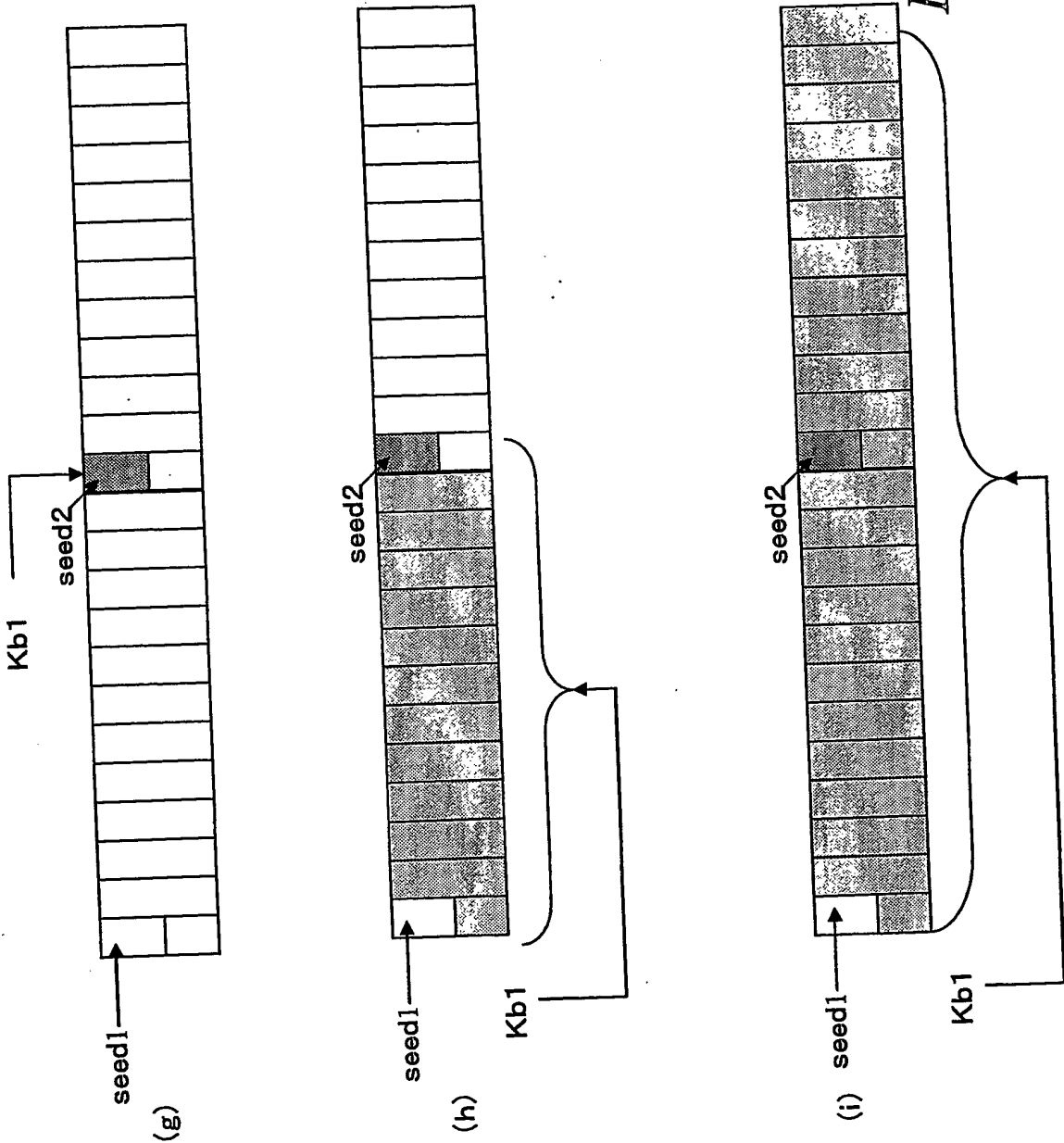


Fig.15

16/23

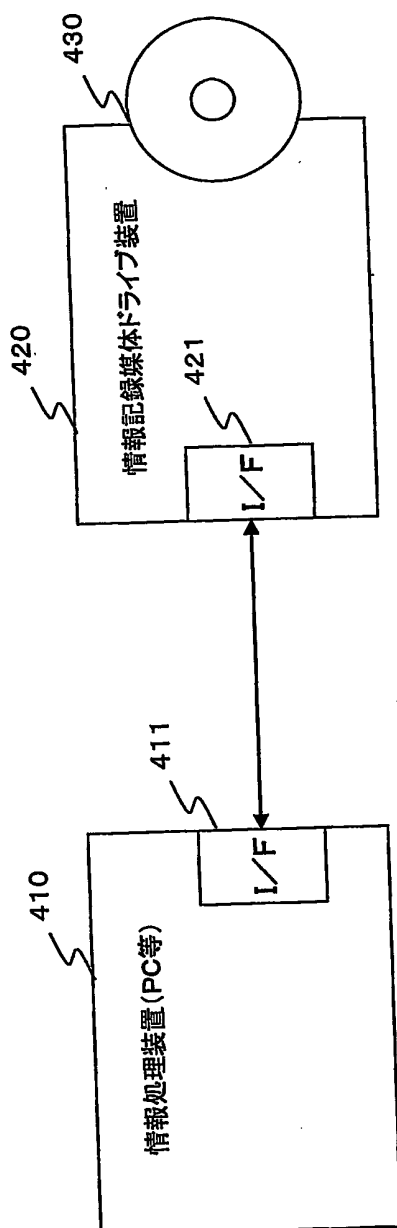
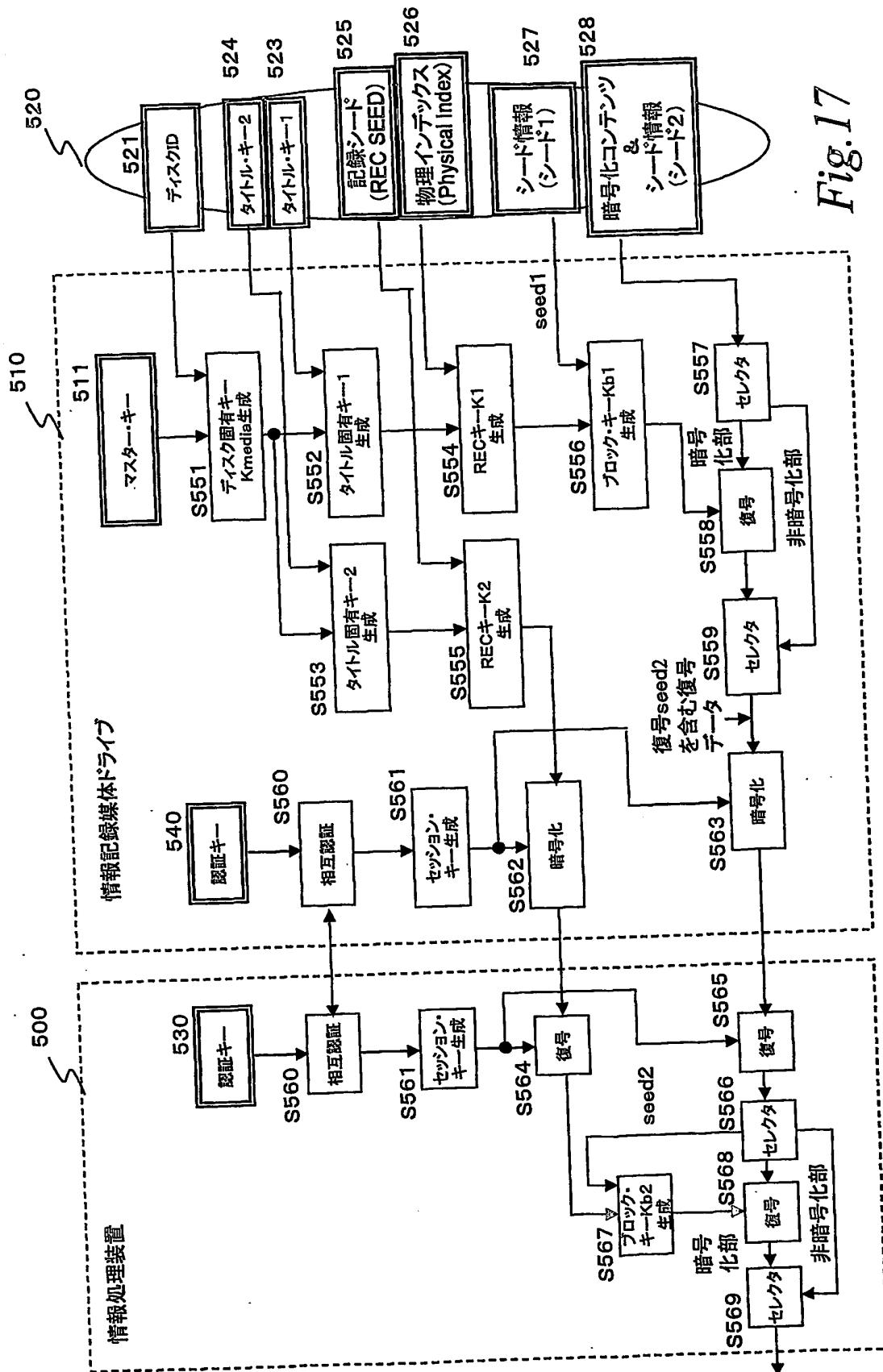


Fig. 16

17/23



19/23

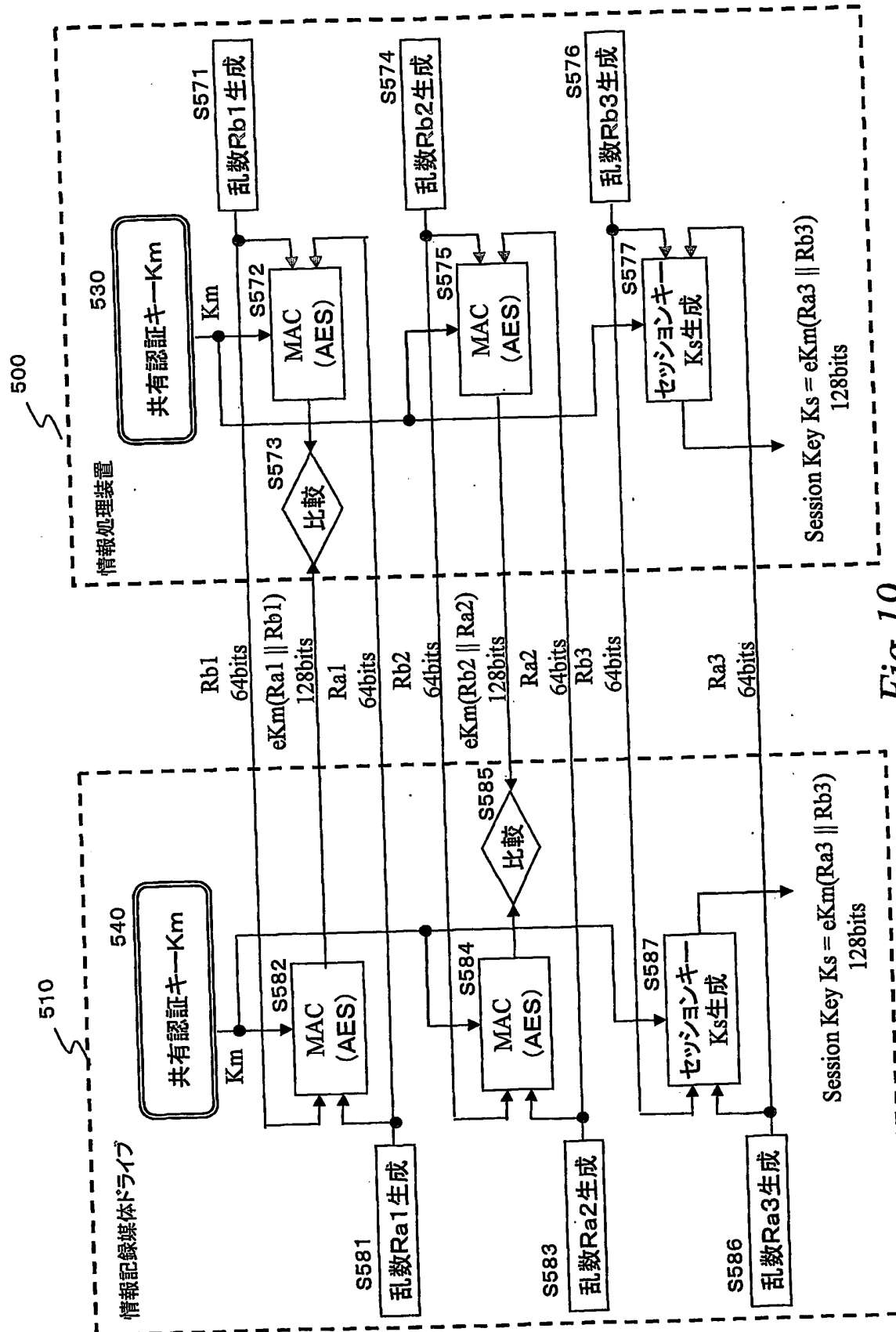
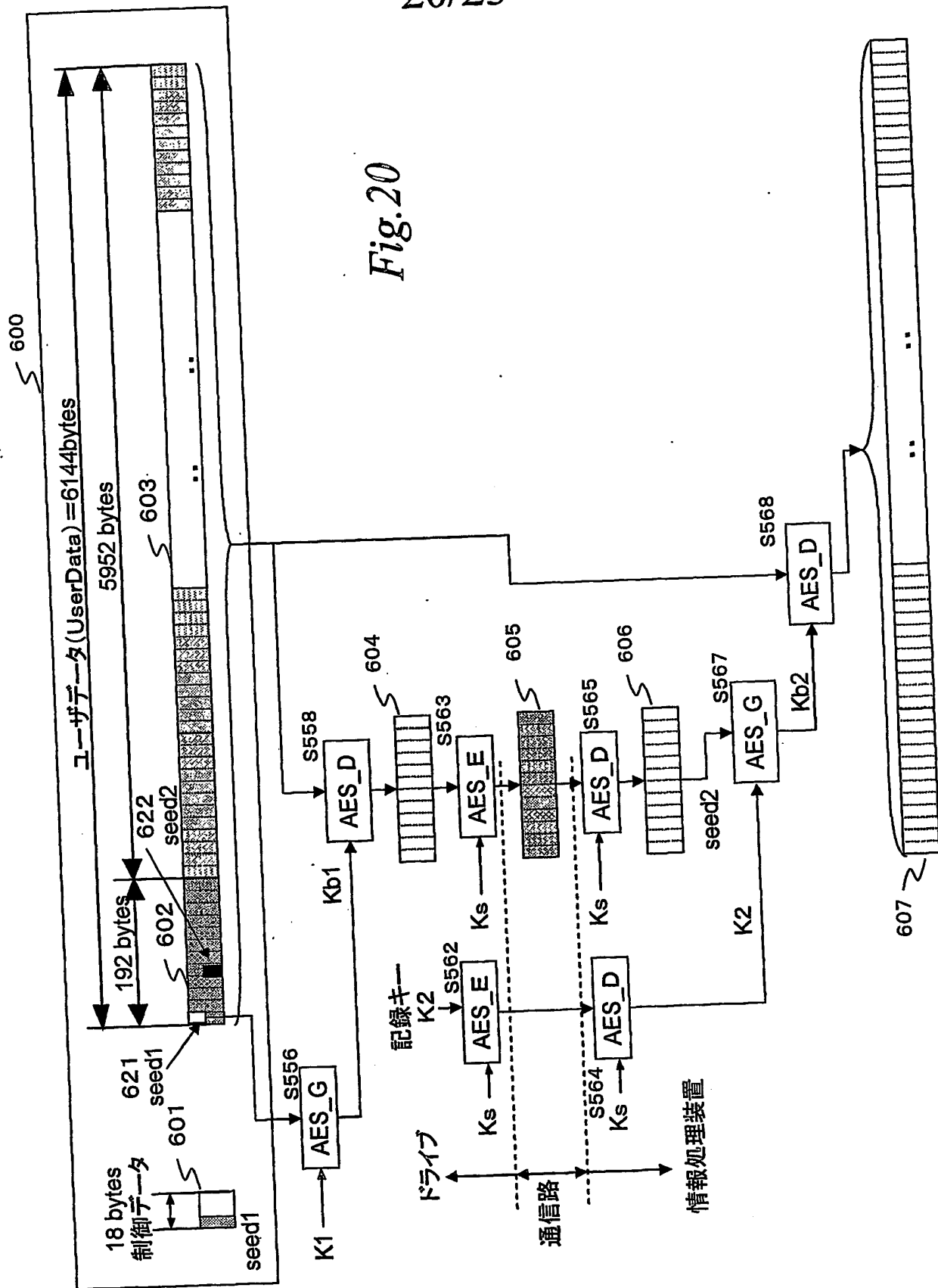
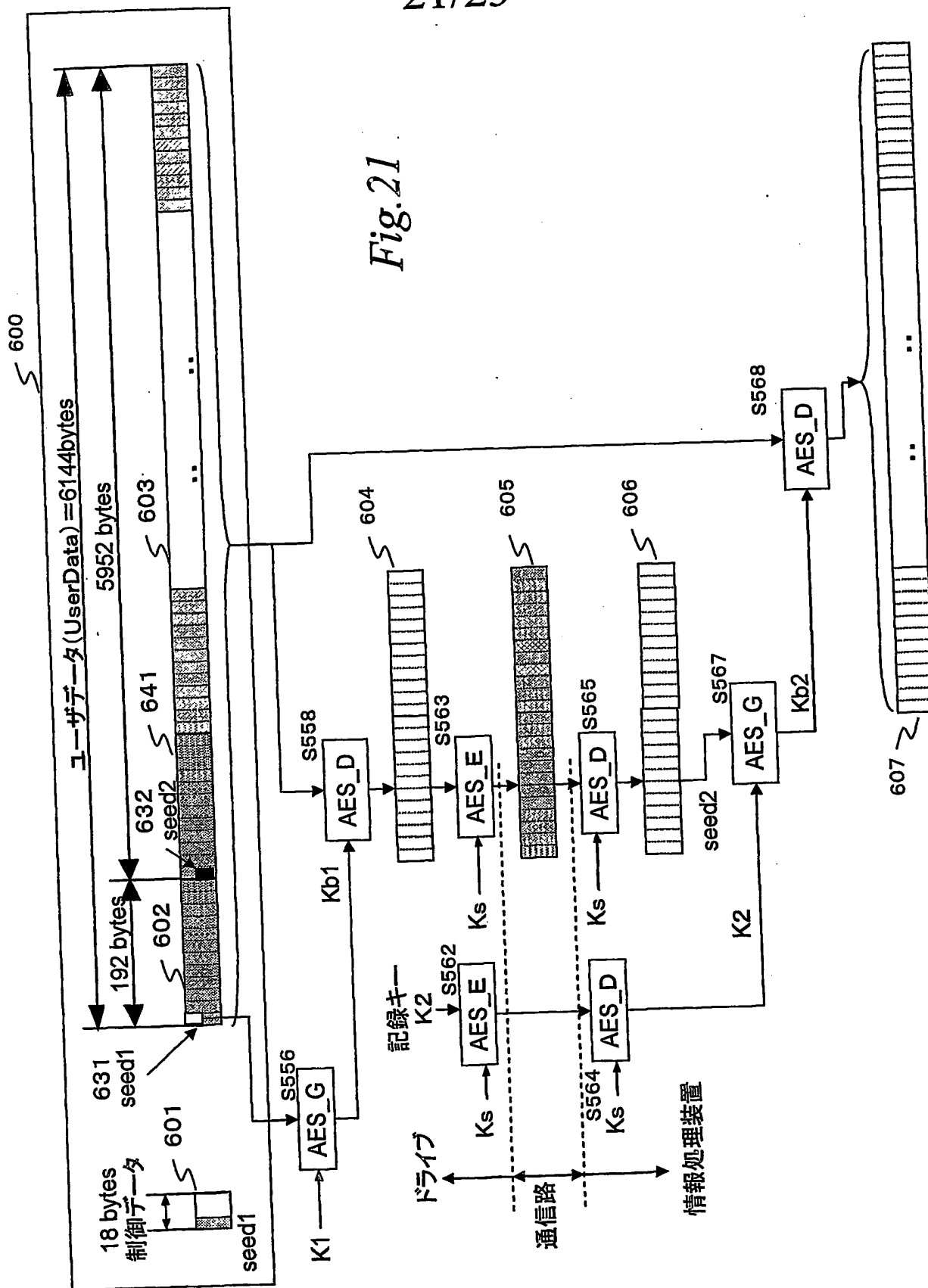


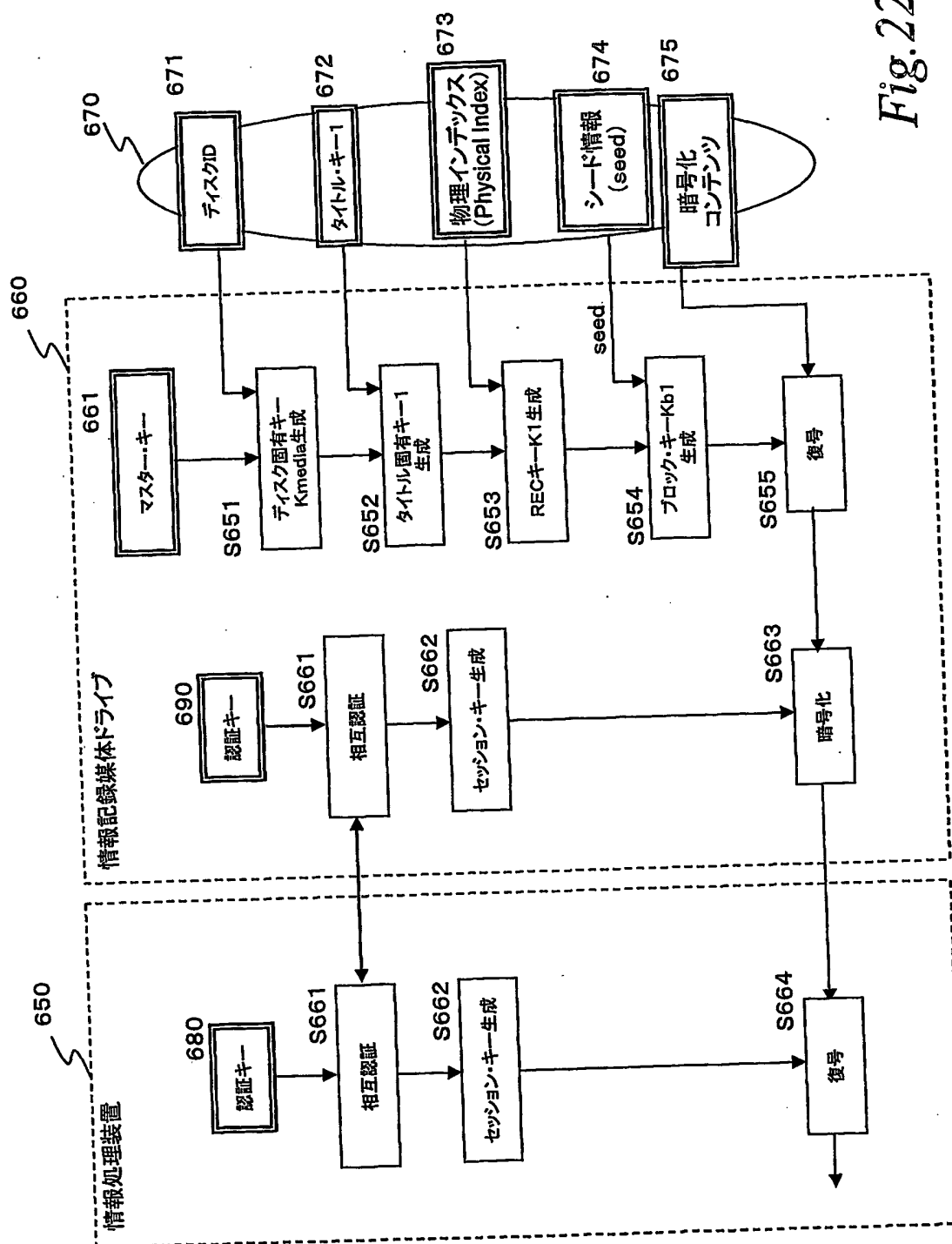
Fig.19



21/23



22/23



23/23

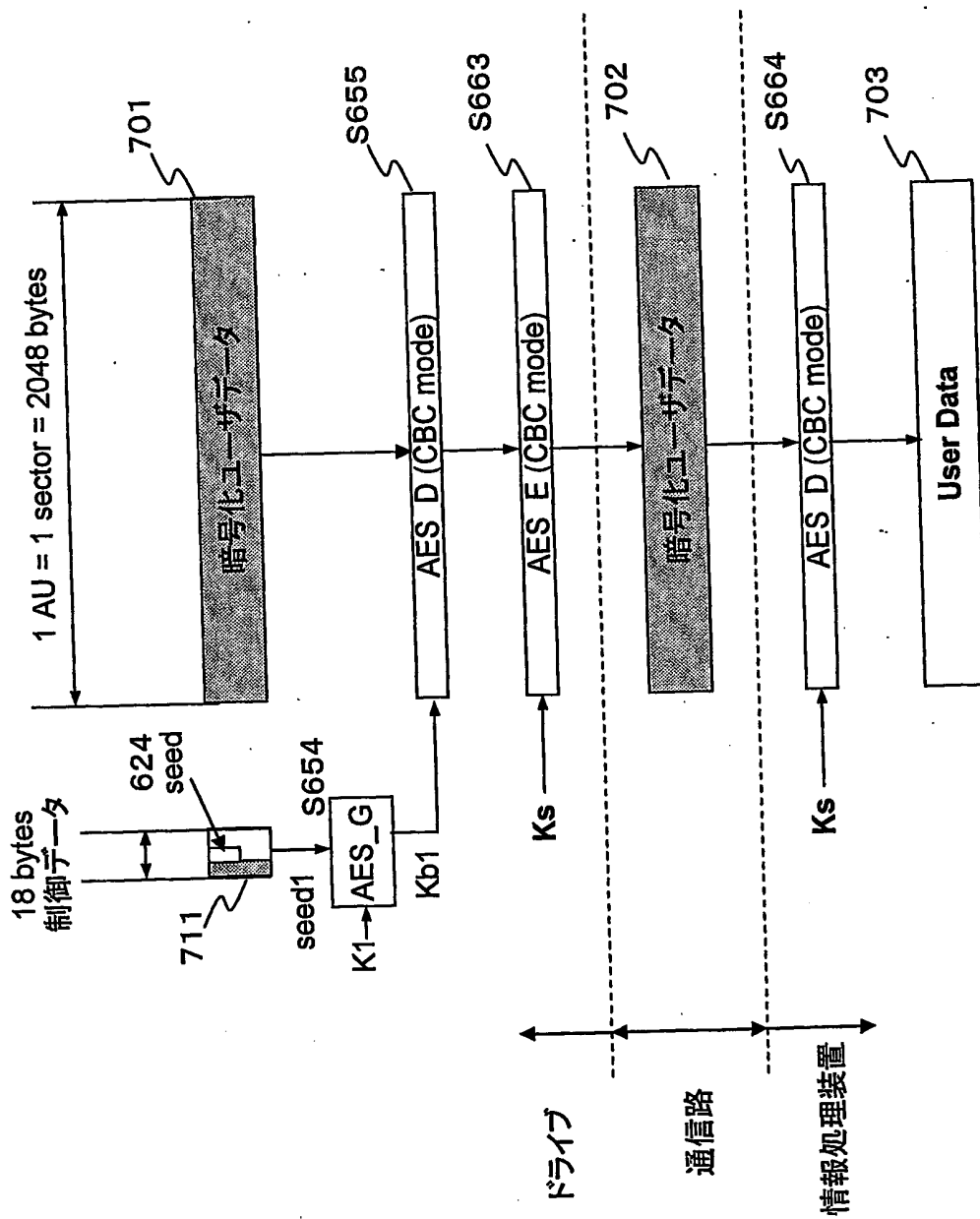


Fig. 23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/004909

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-351324 A (Sony Corp.), 21 December, 2001 (21.12.01), Fig. 21 & EP 1185020 A	7, 8, 20, 21
Y	JP 2000-331420 A (Sony Corp.), 30 November, 2000 (30.11.00), Fig. 20 & EP 1039462 A	7, 8, 20, 21
Y	JP 2002-196982 A (Toshiba Corp.), 12 July, 2002 (12.07.02), Fig. 4 (Family: none)	7, 8, 20, 21

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search
03 June, 2004 (03.06.04)

Date of mailing of the international search report
22 June, 2004 (22.06.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/004909

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-50745 A (Sony Corp.), 21 February, 2003 (21.02.03), Fig. 25 & EP 1291867 A	7, 8, 20, 21
A	JP 10-283270 A (Fujitsu Ltd.), 23 October, 1998 (23.10.98), Full text (Family: none)	1-22

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2004年
 日本国登録実用新案公報 1994-2004年
 日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2001-351324 A (ソニー株式会社) 2001. 12. 21, 第21図 & EP 1185020 A	7, 8, 20, 21
Y	JP 2000-331420 A (ソニー株式会社) 2000. 11. 30, 第20図 & EP 1039462 A	7, 8, 20, 21
Y	JP 2002-196982 A (株式会社東芝) 2002. 07. 12, 第4図 (ファミリーなし)	7, 8, 20, 21

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

03. 06. 2004

国際調査報告の発送日

22. 6. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA / JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石田 信行

5M

9469

電話番号 03-3581-1101 内線 3598

C (続き) . 関連すると認められる文献

引用文献の
カテゴリー*

引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示

関連する
請求の範囲の番号

Y

JP 2003-50745 A (ソニー株式会社)
2003. 02. 21, 第25図 & EP 1291867 A

7, 8, 20, 21

A

JP 10-283270 A (富士通株式会社)
1998. 10. 23, 全文 (ファミリーなし)

1 - 22

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl. H04L9/08

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl. H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2004年
 日本国登録実用新案公報 1994-2004年
 日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 2001-351324 A (ソニー株式会社) 2001. 12. 21, 第21図 & EP 1185020 A	7, 8, 20, 21
Y	J P 2000-331420 A (ソニー株式会社) 2000. 11. 30, 第20図 & EP 1039462 A	7, 8, 20, 21
Y	J P 2002-196982 A (株式会社東芝) 2002. 07. 12, 第4図 (ファミリーなし)	7, 8, 20, 21

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

- の日の後に公表された文献
 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

03. 06. 2004

国際調査報告の発送日

22. 6. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石田 信行

5M

9469

電話番号 03-3581-1101 内線 3598

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2003-50745 A (ソニー株式会社) 2003. 02. 21, 第25図 & EP 1291867 A	7, 8, 20, 21
A	JP 10-283270 A (富士通株式会社) 1998. 10. 23, 全文 (ファミリーなし)	1 - 22